Addonics iSCSI Subsystem

ISC8P2G

User Manual

Table of Contents

Chapter 1 RAID introduction 4
1.1 Features 4
1.2 Terminology 5
1.3 RAID levels 7
Chapter 2 Getting started 9
2.1 Before starting 9
2.2 iSCSI introduction 9
2.3 Management methods 11
2.3.1 Web GUI 11
2.3.2 Console serial port 12
2.3.3 Remote control – secure shell 12
2.4 Enclosure 12
2.4.1 LCM 12
2.4.2 System buzzer 14
2.4.3 LED 15
Chapter 3 Web GUI guideline 16
3.1 P-series GUI hierarchy 16
3.2 Login 17
3.3 Quick install 19
3.4 System configuration 20
3.4.1 System name 21
3.4.2 IP address 21
3.4.3 Language 22
3.4.4 Login config 22
3.4.5 Password 23
3.4.6 Date 23
3.4.7 Mail 24
3.4.8 SNMP 25
3.4.9 Messenger 25
3.4.10 System log server 26
3.4.11 Event log 26
3.5 iSCSI config 27
3.5.1 Entity property 28
3.5.2 NIC 28
3.5.3 Node 29
3.5.4 Session 29
3.5.5 CHAP account 30
3.6 Volume configuration 31
3.6.1 Volume relationship diagram 31
3.6.2 Physical disk 32
3.6.3 Volume group 35
3.6.4 User data volume 36
3.6.5 Cache volume 38
3.6.6 Logical unit number 39

3.6.7 Examples 41
3.7 Enclosure management 51
3.7.1 SES configuration 51
3.7.2 Hardware monitor 52
3.7.3 Hard drive S.M.A.R.T. function support 53
3.7.4 UPS 54
3.8 System maintenance 55
3.8.1 Upgrade 56
3.8.2 Info 56
3.8.3 Reset to default 57
3.8.4 Config import & export 57
3.8.5 Shutdown 58
3.9 Logout 58
Chapter 4 Advanced operation 59
4.1 Rebuild 59
4.2 VG migration and expansion 61
4.3 UDV Extension 64
4.7 Support Microsoft MPIO and MC/S 65
Appendix 66
A. Certification list 66
B. Event notifications 68
C. Known issues 72
D. Microsoft iSCSI Initiator 73
E. MPIO and MC/S setup instructions 78
F. QLogic QLA4010C setup instructions 99
G. Installation Steps for Large Volume (TB) 104

Chapter 1 RAID Introduction

1.1 Features

The **Addonics ISC8P2G iSCSI subsystem** is a high-performance hardware RAID controller.

- RAID 6 ready.
- SATA II support and SATA I backward compatible.
- N-way mirror.
- On-line volume expansion and RAID level migration.
- Global/dedicated cache configuration by volume.
- S.M.A.R.T. enabled.
- Support SES.
- Disk roaming.
- MPIO ready (initiator driver support needed).
- MC/S ready (initiator driver support needed).
- Support iSCSI header and data digest.
- Support CHAP authentication.

With proper configuration, ISC8P2G iSCSI subsystem can provide non-stop service with a high degree of fault tolerance using RAID technology and advanced array management features.

The ISC8P2G iSCSI subsystem connects to the host system via iSCSI interface. It can be configured to any RAID level. ISC8P2G provides reliable data protection for servers using **RAID 6**. RAID 6 allows two HDD failures without any impact on the existing data. Data can be recovered from the remaining data and parity drives.

The ISC8P2G iSCSI subsystem is the most cost-effective disk array controller with completely integrated high-performance and data-protection capabilities which meet or exceed the highest industry standards. **The best data solution for small/medium business (SMB) users.**

1.2 Terminology

The document uses the following terms:

RAID	RAID is the abbreviation of **"R**edundant **A**rray of **I**ndependent **D**isks**"**. There are different RAID levels with different degree of data protection, data availability, and performance to the host environment.
PD	The **P**hysical **D**isk is a member disk of one specific volume group.
VG	**V**olume **G**roup. A collection of removable media. One VG consists of a set of UDVs and owns one RAID level attribute.
UDV	**U**ser **D**ata **V**olume. Each VG could be divided into several UDVs. The UDVs from one VG share the same RAID level, but may have different volume capacity.
CV	**C**ache **V**olume. ISC8P2G uses the on board memory as cache. All RAM (except for the part which is occupied by the controller) can be used as cache. User can divide the cache for one UDV or share among all UDVs. Each UDV will be associated with one CV for data transaction. Each CV could be assigned different cache memory sizes.
LUN	**L**ogical **U**nit **N**umber. A logical unit number (LUN) is a unique identifier used on an iSCSI connection which enables it to differentiate among separate devices (each of which is a logical unit).
GUI	**G**raphical **U**ser **I**nterface.
RAID width, RAID copy, RAID row (RAID cell in one row)	RAID width, copy and row are used to describe one VG. E.g.: 1. One 4-disk RAID 0 volume: RAID width= 4; RAID copy=1; RAID row=1. 2. One 3-way mirroring volume: RAID width=1; RAID copy=3; RAID row=1. 3. One RAID 10 volume over 3 4-disk RAID 1 volume: RAID width=1; RAID copy=4; RAID row=3.

WT	**W**rite-**T**hrough cache write policy. A caching technique in which the completion of a write request is not signaled until data is safely stored on non-volatile media. Each data is synchronized in both data cache and the accessed physical disks.
WB	**W**rite-**B**ack cache write policy. A caching technique in which the completion of a write request is signaled as soon as the data is in cache and actual writing to non-volatile media occurs at a later time. It speeds up system write performance but bears the risk where data may be inconsistent between data cache and the physical disks in one short time interval.
RO	Set the volume to be **R**ead-**O**nly.
DS	**D**edicated **S**pare disks. The spare disks are only used by one specific VG. Others could not use these dedicated spare disks for any rebuilding purposes.
GS	**G**lobal **S**pare disks. GS is shared for rebuilding purpose. If some VGs need to use the global spare disks for rebuilding, they could get the spare disks out from the common spare disks pool for such requirement.
DC	**D**edicated **C**ache.
GC	**G**lobal **C**ache.
DG	**D**e**G**raded mode. Not all of the array's member disks are functioning, but the array is able to respond to application read and write requests to its virtual disks.
S.M.A.R.T.	**S**elf-**M**onitoring **A**nalysis and **R**eporting **T**echnology.
WWN	**W**orld **W**ide **N**ame.
HBA	**H**ost **B**us **A**dapter.
MPIO	**M**ulti-**P**ath **I**nput/**O**utput.
MC/S	**M**ultiple **C**onnections per **S**ession
S.E.S	**S**CSI **E**nclosure **S**ervices.

NIC	**N**etwork **I**nterface **C**ard.
iSCSI	**I**nternet **S**mall **C**omputer **S**ystems **I**nterface.
MTU	**M**aximum **T**ransmission **U**nit.
CHAP	**C**hallenge **H**andshake **A**uthentication **P**rotocol. An optional security mechanism to control access to an iSCSI storage system over the iSCSI data ports.
iSNS	**I**nternet **S**torage **N**ame **S**ervice.

1.3 RAID levels

RAID 0	Disk striping. ISC8P2G RAID 0 needs at least two hard drives.
RAID 1	Disk mirroring over two disks. RAID 1 needs at least two hard drives.
N-way mirror	Extension to RAID 1 level. It has N copies of the disk.
RAID 3	Striping with parity on the dedicated disk. RAID 3 needs at least three hard drives.
RAID 5	Striping with interspersed parity over the member disks. RAID 5 needs at least three hard drives.
RAID 6	2-dimensional parity protection over the member disks. RAID 6 needs at least four hard drives.
RAID 0+1	Mirroring of the member RAID 0 volumes. RAID 0+1 needs at least four hard drives.
RAID 10	Striping over the member RAID 1 volumes. RAID 10 needs at least four hard drives.
RAID 30	Striping over the member RAID 3 volumes. RAID 30 needs at least six hard drives.

RAID 50	Striping over the member RAID 5 volumes. RAID 50 needs at least six hard drives.
RAID 60	Striping over the member RAID 6 volumes. RAID 60 needs at least eight hard drives.
JBOD	The abbreviation of **"J**ust a **B**unch **O**f **D**isks**"**. JBOD needs at least one hard drive.

Chapter 2 Getting started

2.1 Before starting

Before starting, prepare the following items.

1. Check the **“Certification list”** in Appendix A to confirm the hardware setting is fully supported.
2. A server or worksation with a NIC or iSCSI HBA.
3. CAT 5e, or CAT 6 network cables for web GUI IP port and iSCSI data ports. We recommend CAT 6 cables for best performance.
4. Prepare storage system configuration plan.
5. Management (web GUI IP port) and iSCSI data ports network information. When using static IP, please prepare static IP addresses, subnet mask, and default gateway.
6. Gigabit LAN switches. (Recommended)
7. CHAP security information, including CHAP usernames and secrets. (Optional)
8. Setup the hardware connection before powering up servers and ISC8P2G iSCSI subsystem. Connect web GUI IP port cable, and iSCSI data port cables first.

2.2 iSCSI introduction

iSCSI (Internet SCSI) is a protocol which encapsulates SCSI (Small Computer System Interface) commands and data in TCP/IP packets for linking storage devices with servers over common IP infrastructures. iSCSI provides high performance SANs over standard IP networks like LAN, WAN or the Internet.

IP SANs are true SANs (Storage Area Networks) which allow servers to attach to an infinite number of storage volumes by using iSCSI over TCP/IP networks. IP SANs can scale the storage capacity with any type and brand of storage system. IP-SANs also include mechanisms for security, data replication, multi-path and high availability.

Storage protocol, such as iSCSI, has “two ends” in the connection. These ends are the initiator and the target. In iSCSI we call them iSCSI initiator and iSCSI target. The iSCSI initiator requests or initiates any iSCSI communication. It requests all SCSI operations like read or write. An initiator is usually located on the host/server side (either an iSCSI HBA or iSCSI Software initiator).

The iSCSI target is the storage device itself or an appliance which controls and serves volumes or virtual volumes. The target is the device which performs SCSI commands or bridges it to an attached storage device. iSCSI targets can be disks, tapes, RAID arrays, tape libraries, and etc.

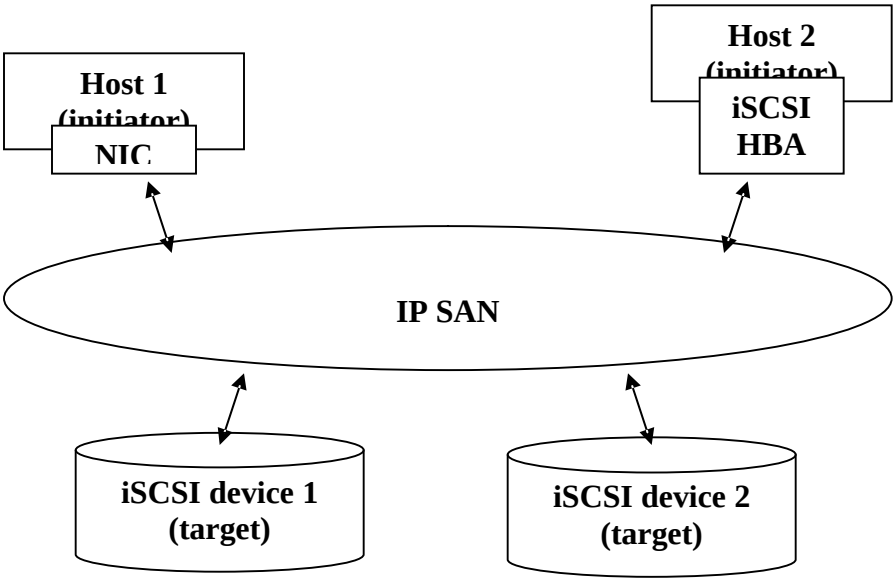


Figure 2.2.1

The host side needs an iSCSI initiator. The initiator is a driver which handles the SCSI traffic over iSCSI. The initiator can be software or hardware (HBA). Please refer to the certification list of iSCSI HBA(s) in Appendix A. OS native initiators or other software initiators use the standard TCP/IP stack and Ethernet hardware, while iSCSI HBA(s) use their own iSCSI and TCP/IP stacks.

Hardware iSCSI HBA(s) would provide its initiator tool. Please refer to the vendors' HBA user manual. **Microsoft**, **Linux** and **Mac** provide software iSCSI initiator driver. Below are the available links:

1. Link to download the Microsoft iSCSI software initiator: http://www.microsoft.com/downloads/details.aspx?familyid=12cb3c1a-15d6-4585-b385-befd1319f825&displaylang=en

   Please refer to Appendix D for Microsoft iSCSI initiator installation procedure.

2. Linux iSCSI initiator is also available. For different kernels, there are different iSCSI drivers. Please check Appendix A for software iSCSI initiator certification list. If user needs the latest Linux iSCSI initiator, please visit Open-iSCSI project for most update information. Linux-iSCSI (sfnet) and Open-iSCSI projects merged in April 11, 2005.

Open-iSCSI website: http://www.open-iscsi.org/
Open-iSCSI README: http://www.open-iscsi.org/docs/README
Google groups:
http://groups.google.com/group/open-iscsi/threads?gvc=2
http://groups.google.com/group/open-iscsi/topics

3. globalSAN iSCSI Initiator for OS X
http://www.studionetworksolutions.com/products/product_detail.php?t=more&pi=11
ATTO iSCSI initiator is available for Mac.
Website: http://www.attotech.com/xtend.html

2.3 Management methods

There are three management methods to manage ISC8P2G iSCSI subsystem:

2.3.1 Web GUI

ISC8P2G supports graphical user interface (GUI) to manage the system. The default setting of the web GUI port IP is DHCP and the DHCP IP address is displayed on the LCM. A user can check the LCM for the IP addres first, then open a web browser and type the DHCP address: (The DHCP address is dynamic and user may need to check every time after reboot again.)
E.g., on LCM.

192.168.1.50
Addonics ISC8P2G
•

http://192.168.1.50

Move the cursor on any of the function block located on the left side of the web browser, a dialog box opens to authenticate current user.

Login name: **admin**
Default password: **supervisor**

Or login with the read-only account which only allows seeing the configuration and cannot change setting.

Login name: **user**
Default password: **1234**

2.3.2 Console serial port (Optional)

Use NULL modem cable to connect console port.
The console setting is baud rate: **115200**, 8 bits, 1 stop bit, and no parity.
Terminal type: **vt100**
Login name: **admin**
Default password: **supervisor**

2.3.3 Remote control – secure shell

SSH (secure shell) is required for ISC8P2G to remote login. The SSH client software is available at the following web site:
SSHWinClient WWW: http://www.ssh.com/
Putty WWW: http://www.chiark.greenend.org.uk/

Host name: **192.168.1.50 (Please check your DHCP address for this field.)**
Login name: **admin**
Default password: **supervisor**

E.g.
$ ssh admin@192.168.1.50

Tips
ISC8P2G only support SSH for remote control. When using SSH, the IP address and the password is required for login.

2.4 Enclosure

2.4.1 LCM

There are four buttons to control **ISC8P2G** LCM (LCD Control Module), including:
• (up), , (down), **ESC** (Escape), and **ENT** (Enter).

After booting up the system, the following screen shows web GUI port IP and model name:

192.168.1.50
Addonics ISC8P2G•

Press **“ENT”**.

The following are LCM functions: **“Alarm Mute”**, **“Reset/Shutdown”**, **“Quick Install”**, **“View IP Setting”**, **“Change IP Config”** and **“Reset to Default”**. To shift between the menus, press • (up) or , (down) buttons.

When a WARNING or ERROR is detected within the device, the LCM displays the event log to provide users more details.

The following table shows each function’s description.

Alarm Mute	To mute the alarm when an error occurs, select this function.
Reset/Shutdown	To reset or shutdown the ISC8P2G.
Quick Install	Three Quick steps to create a volume. Please refer to section 3.3 for procedure using the web GUI.
View IP Setting	Display current IP address, subnet mask, and gateway.
Change IP Config	Set IP address, subnet mask, and gateway. There are 2 selections, DHCP (Get IP address from DHCP server) or set static IP.
Reset to Default	Reset to default sets password to default: **supervisor**, and set IP address to default as DHCP setting. Example: Default IP address: **192.168.1.50 (DHCP)** Default subnet mask: **255.255.255.0** Default gateway: **192.168.1.254**

The following is LCM menu hierarchy.

ADDONICS Technology • ,	[Alarm Mute]	[• Yes No ,]		
	[Reset/Shutdown]	[Reset]	[• Yes No ,]	
		[Shutdown]	[• Yes No ,]	
	[Quick Install]	RAID 0 (RAID 1/RAID 3/ RAID 5/RAID 6) xxxxxx GB	Volume Size (xxxxxx G)	Adjust Volume Size
			Apply The Config	[• Yes No ,]
	[View IP Setting]	[IP Config] [Static IP]		
		[IP Address] [192.168.001.050]		
		[IP Subnet Mask] [255.255.255.0]		
		[IP Gateway] [192.168.001.254]		
	[Change IP Config]	[DHCP]	[• Yes No ,]	
		[Static IP]	[IP Address]	Adjust IP address
			[IP Subnet Mask]	Adjust Submask IP
			[IP Gateway]	Adjust Gateway IP
			[Apply IP Setting]	[• Yes No ,]
	[Reset to Default]	[• Yes No ,]		

Caution
Before powering off, it is recommended to execute **"Shutdown"** to flush the data from cache to physical disks.

2.4.2 System buzzer

The system buzzer features are describe in the following:

1. The system buzzer alarms for 1 second when system boots up successfully.
2. The system buzzer alarms continuously when an error event happens. To stop the alarm, use the alarm mute option.
3. The alarm will be muted automatically when the error situation is resolved. E.g., when a RAID 5 array is degraded and the alarm rings. After a user changes/adds one physical disk for rebuilding, and when the rebuilding is done, the alarm will be muted automatically.

2.4.3 LED

The LED features are describe as follows:

1. **POWER LED**: Hardware activated LED when system is powered on.
2. **BUSY LED**: Hardware activated LED when the front-end channel is busy.
3. **System STATUS LED**: Indicates system status. When an error occurs or the RAID is degraded, the LED lights up.

Chapter 3 Web GUI guideline

3.1 ISC8P2G Web GUI Hierarchy

The table below shows the hierarchy of ISC8P2G Web GUI.

Quick Install	à	Step 1 / Step 2 / Step 3 / Confirm
System Config		
System name	à	System name
IP address	à	DHCP / Static / Address / Mask / Gateway / DNS / HTTP port / HTTPS port / SSH port
Language	à	Language
Login config	à	Auto logout / Login lock
Password	à	Old password / Password / Confirm
Date	à	Time zone / Date / Time / NTP Server
Mail	à	Mail-from address / Mail-to address / Sent events / SMTP relay / SMTP server / Authentication / Account / Password / Confirm / Send test mail
SNMP	à	SNMP trap address / Community / Send events
Messenger	à	Messenger IP/hostname / Send events
System log server	à	Server IP/hostname / Port / Facility / Event level
Event log	à	Filter / Download / Mute / Clear
iSCSI config		
Entity Property	à	Entity name / iSNS IP
NIC	à	Aggregation / IP settings for iSCSI ports / Become default gateway / Set MTU
Node	à	Change Authentication
Session	à	Delete
CHAP account	à	Create /Delete
Volume config		
Physical disk	à	Free disks / Global spares / Dedicated spares / More information / Auto Spindown
Volume group	à	Create / Delete / More information / Rename / Migrate
User data Volume	à	Attach / Snapshot / Create / Delete / More information / Rename / Extend / Set read/write mode / Set priority / Resize Snapshot space / Auto Snapshot
Cache volume	à	Create / Delete / More information / Resize
Logical unit	à	Attach / Detach
Enclosure management		
SES config	à	Enable / Disable
Hardware monitor	à	Auto shutdown
S.M.A.R.T.	à	**(Only for SATA disks)**
UPS	à	UPS Type / Shutdown Battery Level / Shutdown Delay / Shutdown UPS

Maintenance

Upgrade	à	Browse the firmware to upgrade / Export config
Info	à	System information
Reset to default	à	Sure to reset to factory default?
Config import &export	à	Import/Export / Import file
Shutdown	à	Reboot / Shutdown

Logout Sure to logout?

3.2 Login

On the web browser, type the IP address shown on the LCM display.

Figure 3.2.1

Place the cursor on any function block located on the left side of window then do a right click, an authentication window opens up.

Connect to 192.168.1.4
The server 192.168.1.4 at Authentication: 67c7c469ac33e67684cf6349ce596a4b requires a username and password.
Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).
User name:
Password:
Remember my password
OK
Cancel

Figure 3.2.2

User name: admin
Password: supervisor

After login, you can choose the Quick Install function block on the left side of the window to do configuration.

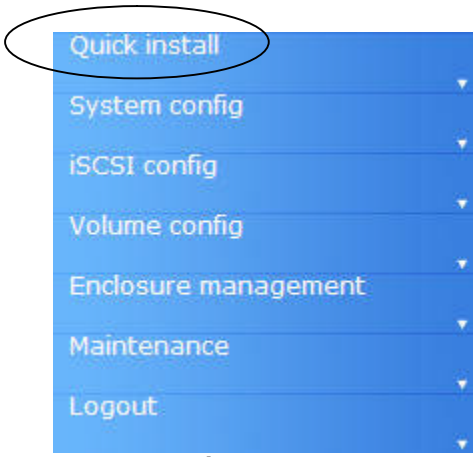


Figure 3.2.3

There are four indicators at the top-right corner of the web GUI.

Figure 3.2.4

1. **RAID light:** Green means, the RAID array is correctly functioning. Red represents RAID failure or degradation.

2. **Temperature light:** Green is normal. Red represents abnormal temperature.

3. **Voltage light:** Green is normal. Red represents abnormal voltage status.

4. **UPS light:** Green is normal. Red represents abnormal UPS status.

3.3 Quick Install

The “Quick install” function is used to create a volume.

The ISC8P2G Quick Install function has a smart policy. When the system is full, meaning all 8 HDD are connected, and all HDD have the same size, ISC8P2G’s Quick Install function lists all possible configurations and sizes among different RAID level options. The ISC8P2G Quick Install will use all available HDD for the RAID level which the user decides.

But when the system is inserted with different sizes of HDD, e.g., 6*200G HDD and 2*80G, ISC8P2G also lists all possible combinations of different RAID Level and different sizes and you may observe there are some HDD not used (Free Status).

Step 1: Select “Quick install” then choose the RAID level to set. Please refer to Figure 1.2. After choosing the RAID level, click “ Next >> ”, which links to another page, user can set up “LUN” here.

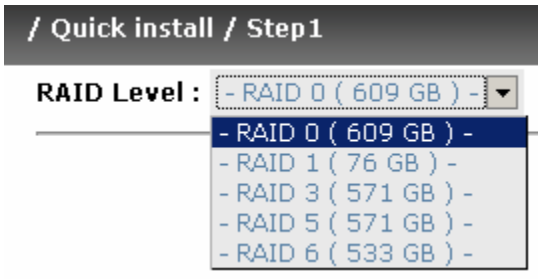


Figure 3.3.1

Step 2: Please select a LUN number. Access control of host would show as a wildcard “*”, which means every host can access this volume. In this page, the “Volume size” can be changed. The maximum volume size is shown. To re-enter the size be sure it has to be less or equal to maximum volume size. Then click “ Next >> ”.

Step 3: Confirm page. Click “ Confirm ” if all setups are correct. Then a page with the “User data volume” just created will be shown as Figure 1.3.

This would complete the iSCSI drive configuration.

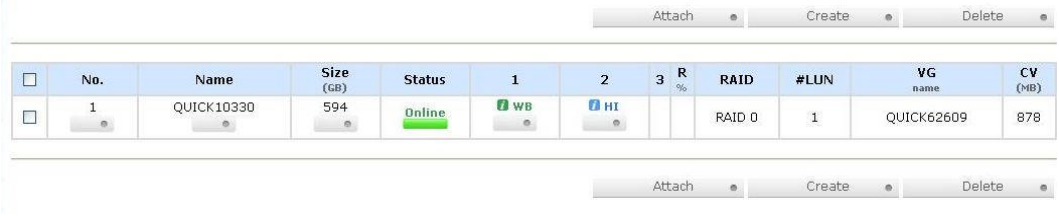


Figure 3.3.2

(Figure 3.3.2: A RAID 0 user data volume with the UDV name “QUICK10330”, named by the system itself, with the total available volume size 594GB.)

3.4 System Configuration

“System config” is used for setting up **“System name”**, **“IP address”**, **“Language”**, **“Login config”**, **“Password”**, **“Date”**, **“Mail”**, **“SNMP”**, **“Messenger”**, **“System log server”** and view **“Event log”**.

System name	System name for identification
IP address	Internet Protocol(IP) address for remote administration
Language	Language preference for WebUI
Login config	Configuration for auto logout and login lock
Password	Administrator's password
Date	System time for event log
Mail	Alert by e-mail
SNMP	Alert via Simple Network Management Protocol(SNMP)
Messenger	Transmits net send and Alerter service messages between clients and servers
System log server	Alert to remote system log server
Event log	System event log to record critical events

Figure 3.4.1

3.4.1 System name

Select **“System name”** to modify system name. The default system name consists of the model name and serial number of this system, e.g.: ISC8P2G-A00001.

Figure 3.4.1.1

Click “ Confirm ” after modifying.

3.4.2 IP address

Select **“IP address”** to change IP address for remote administration usage (web GUI port IP). There are 2 selections, DHCP (Get IP address from DHCP server) or static IP. The default setting is DHCP enabled. User can change the HTTP and SSH port number when the default port number is not allowed on host/server.

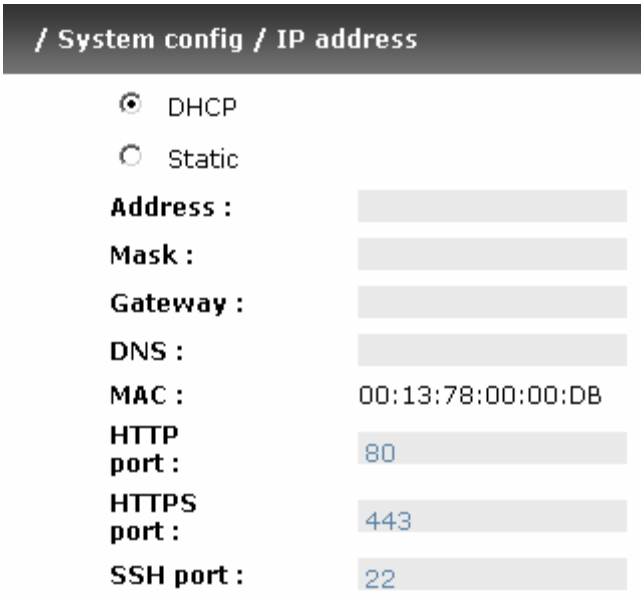


Figure 3.4.2.1

Click “ Confirm ” after modifying.

3.4.3 Language

Select **“Language”** to set the language used in the Web GUI. The option “Auto Detect” will used the browser’s default language setting.

Figure 3.4.3.1

Click “ Confirm ” after modifying.

3.4.4 Login config

Select **“Login config”** to set only one admin and set the auto logout timing. Setting only one admin can prevent multiple users accessing the same IS8P2G at the same time.

1. Auto logout: The options are (1) Disable; (2) 5 mins; (3) 30 mins; (4) 1 hour. The system will log out automatically when there is no user response for a period of time.
2. Login lock: Disable/Enable. When the login lock is enabled, the system allows only one user to login/modify the system settings.

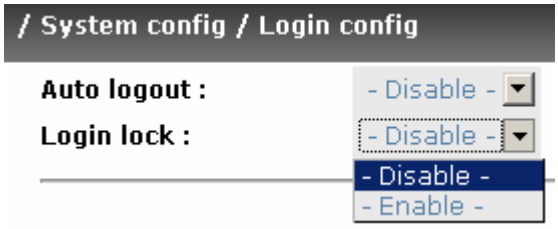


Figure 3.4.4.1

Click “ Confirm ” after modifying.

3.4.5 Password

Select **“Password”** for changing administrator password. The maximum length of admin password is 12 characters.

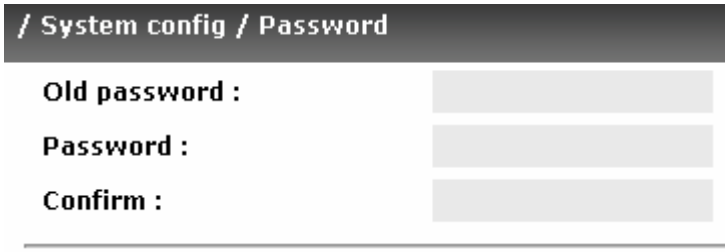


Figure 3.4.5.1

Click “ Confirm ” after modifying.

3.4.6 Date

Select **“Date”** to set up the current date, time, and time zone or synchronize time from NTP(Network Time Protocol) server.

Figure 3.4.6.1

Click “ Confirm ” after modifying.

3.4.7 Mail

Select **“Mail”** to enter at most 3 mail addresses for receiving the event notification. Some mail servers would check **“Mail-from address”** and need authentication. Please fill the necessary fields and select **“Send test mail”** to check whether the email works fine. User can also select which levels of event logs will be sent out by Mail. Default setting is WARNING and ERROR event logs.

Figure 3.4.7.1

Fill out the following parameters:
Mail-from address:
Mail-to address 1:
Click on SMTP relay
SMTP server:
Click on Send test mail:
to test and determine if it is forwarding mail alert to the email address.

Click “ Confirm ” after modifying.

3.4.8 SNMP

Select **"SNMP"** to set up SNMP trap alert via SNMP. It allows up to 3 SNMP trap addresses. Default community setting is "public". User can choose the event log levels and the default value of SNMP is INFO.

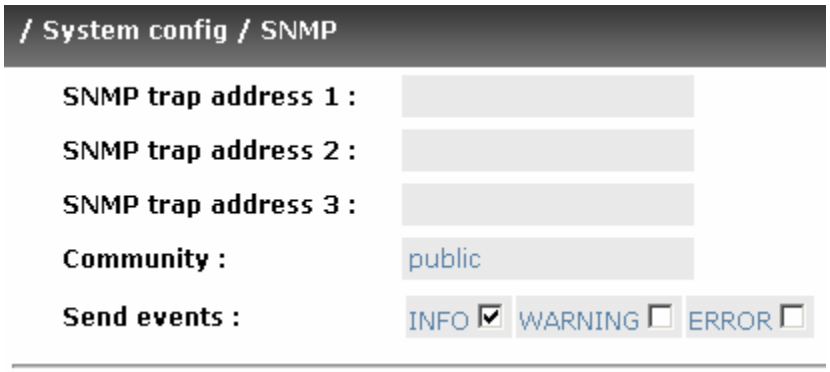


Figure 3.4.8.1

Click "Confirm" after modifying.

There are many SNMP tools. The following web sites are for reference:
SNMPc: http://www.snmpc.com/
Net-SNMP: http://net-snmp.sourceforge.net/

3.4.9 Messenger

Select **"Messenger"** to set up pop-up message alert via Windows messenger (not MSN). User must enable the service "Messenger" in Windows (Start à Control Panel à Administrative Tools à Services à Messenger), and then event logs can be received. It allows up to 3 messenger addresses. User can choose the event log levels and the default values are WARNING and ERROR.

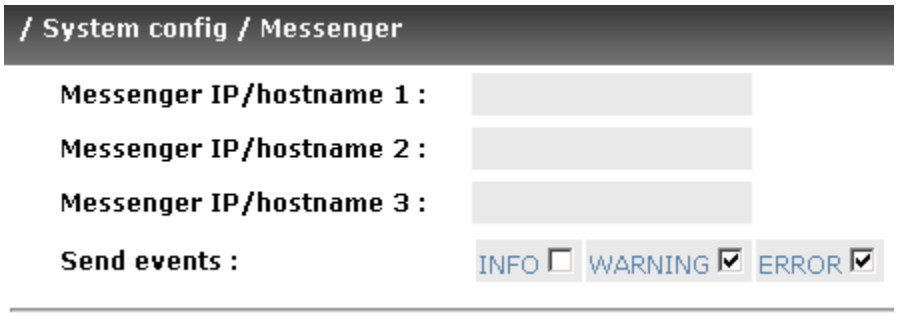


Figure 3.4.9.1

3.4.10 System log server

Select **"System log server"** to set up alert via syslog protocol. The default port of syslog is 514. User can choose the facility and the event log level. The default values of event level are INFO, WARNING and ERROR.

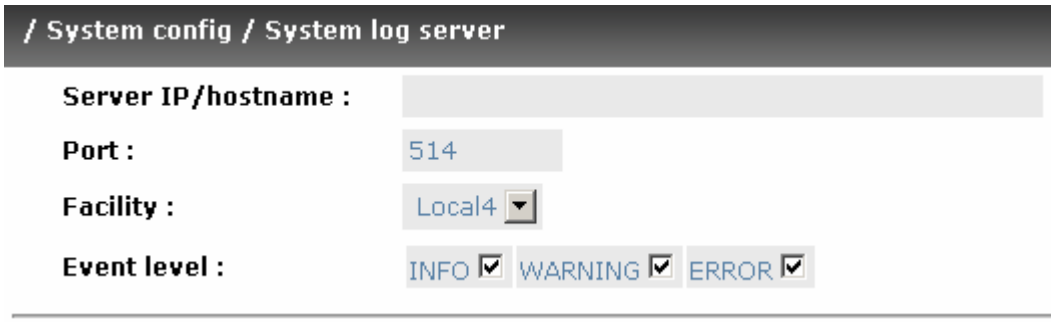


Figure 3.4.10.1

Click "Confirm" after modifying.

There are some syslog server tools. The following web sites are for reference:
WinSyslog: http://www.winsyslog.com/
Kiwi Syslog Daemon: http://www.kiwisyslog.com/
Most UNIX systems build in syslog daemon.

3.4.11 Event log

Select **"Event log"** to view the event messages. Press the **"Filter"** button to choose the display. Press the **"Download"** button to save the whole event log as text file with file name "log-ModelName-SerialNumber-Date-Time.txt" (e.g., log-ISC8P2G-A00001-20070801-120000.txt). Pressing the **"Clear"** button will clear event logs. Pressing the **"Mute"** button will stop alarm if there are system alerts.

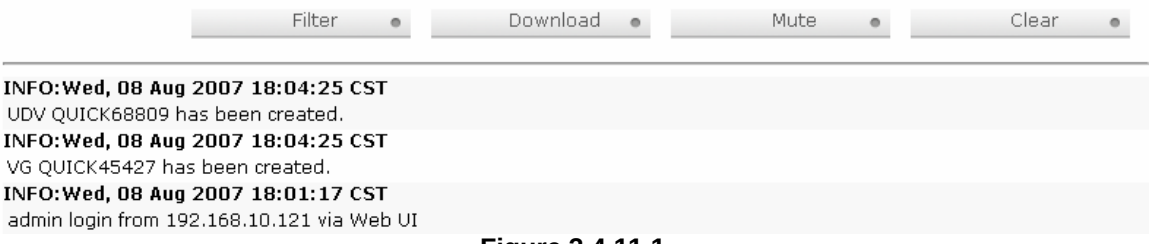


Figure 3.4.11.1

For customizing your own display of event logs, there are a total of three display methods. These are Web UI/Console event log page, popup windows on Web GUI, and on LCM. The default setting of these three displays is WARNING and ERROR. The popup is disabled by default.

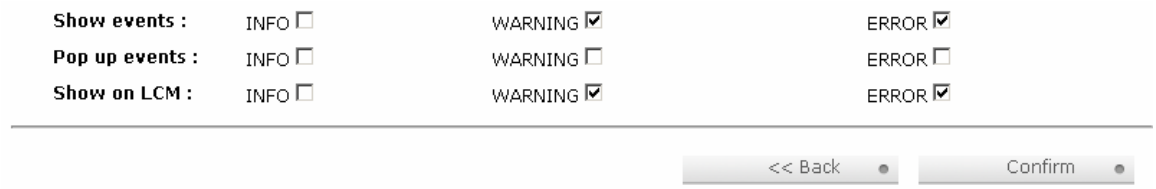


Figure 3.4.11.2

The event log is displayed in reverse order, which means the latest event log is on the first page. The event logs are actually saved in the first four hard drives; each hard drive has one copy of event log. For one ISC8P2G, there are four copies of event logs. This will guarantee access on the event logs even when there is/are failed disk(s).

3.5 iSCSI config

“iSCSI config” selection is for the setup of **“Entity Property”**, **“NIC”**, **“Node”**, **“Session”**, and **“CHAP account”**.

Entity property	iSCSI entity property
NIC	iSCSI portal configuration
Node	iSCSI node configuration
Session	iSCSI session information
CHAP account	Add/Remove account for iSCSI node

Figure 3.5.1

3.5.1 Entity property

Select **“Entity property”** to view the entity name of the ISC8P2G, and setup **“iSNS IP”** for iSNS (Internet Storage Name Service). You can add an iSNS server IP address to the iSNS servers list which the iSCSI initiator service can send queries. The entity name of the ISC8P2G cannot be changed.

Figure 3.5.1.1

3.5.2 NIC

Select **“NIC”** to change IP addresses of iSCSI data ports. The ISC8P2G have two ports.

Name	DHCP	IP address	Netmask	Gateway	Jumbo frame	MAC address	Link
LAN1	Yes	192.168.1.113	255.255.255.0	192.168.1.1	Disabled	00:13:78:04:0f:70	Up
LAN2	Yes	192.168.1.112	255.255.255.0	192.168.1.1	Disabled	00:13:78:04:0f:71	Up

Figure 3.5.2.1

(Figure 3.5.2.1: ISC8P2G, there are 2 iSCSI data ports. MTU is 1500)

User can change IP address by clicking the button “ ” in the **“DHCP”** column. There are 2 selections, DHCP (Get IP address from DHCP server) or static IP.

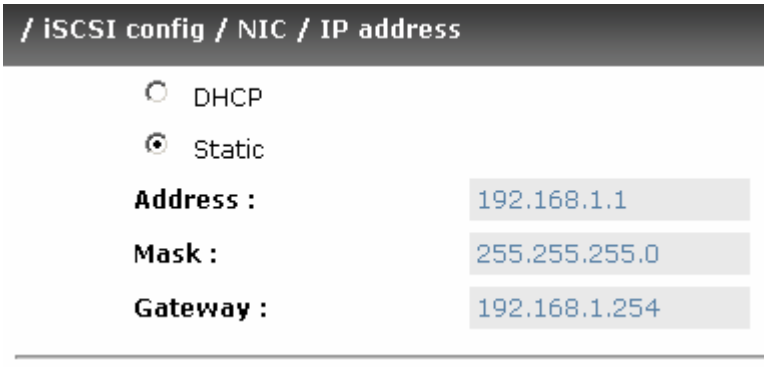


Figure 3.5.2.2

Default gateway can be changed by clicking the button “ ” in the **“Gateway”** column. There is only one default gateway.

3.5.3 Node

Single-node:

Select **“Node”** to view the target name for iSCSI initiator. ISC8P2G supports single-node. The node name of ISC8P2G exists by default and cannot be changed.

Node name	Auth
iqn.1995-07.com.addonics:isc8p2g-000a40f21:default-target	None

Figure 3.5.3.1

3.5.4 Session

Select **“Session”** function. It will display iSCSI session and connection information, including the following items:

1. Host (Initiator Name)
2. Error Recovery Level
3. Error Recovery Count
4. Detail of Authentication status and Source IP: port number.

Delete

	No	Initiator name	TPGT	Error recovery level	Error recovery count
☐	0	iqn.1987-05.com.cisco:01.c047c42de54	0x02	0	0
☐	1	iqn.1987-05.com.cisco:01.c047c42de54	0x02	0	0
☐	2	iqn.1987-05.com.cisco:01.c047c42de54	0x00	0	0

Delete

Figure 3.5.4.1

(Figure 3.5.4.1: iSCSI Session.)

Pressing the button “ ” will display connection(s).

No.	Initiator IP	Initiator name	Authentication
0	192.168.12.212	iqn.1987-05.com.cisco:01.c047c42de54	no

<< Back

Figure 3.5.4.2

(Figure 3.5.4.2: iSCSI Connection.)

3.5.5 CHAP account

Select **“CHAP account”** function to create/delete a CHAP account for authentication. ISC8P2G can create a single CHAP account only.

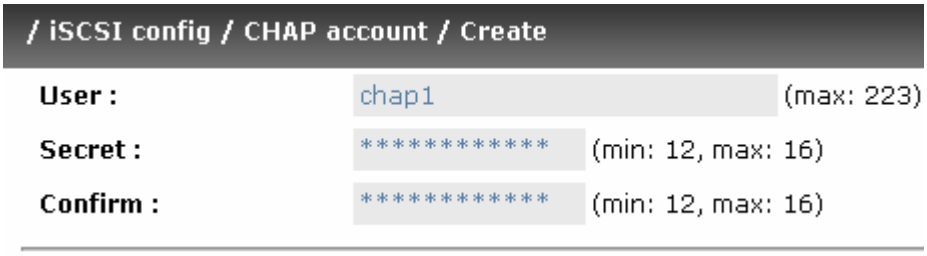


Figure 3.5.5.1

(Figure 3.5.5.1: ISC8P2G, press “Create” to create a CHAP account.)

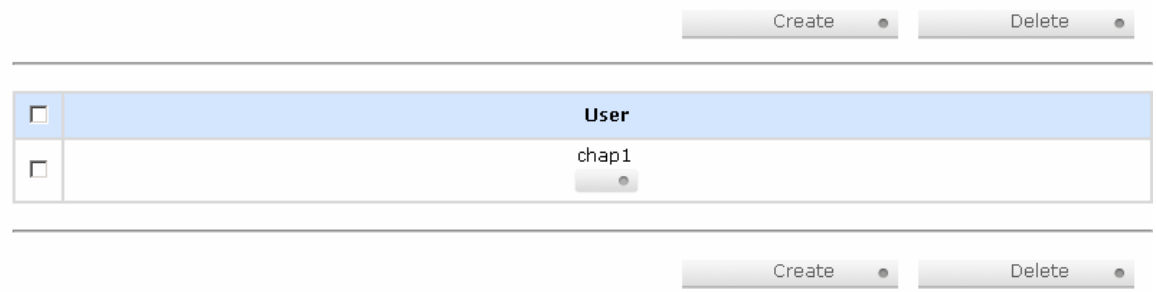


Figure 3.5.5.2

(Figure 3.5.5.2: ISC8P2G, create a CHAP account named “chap1”.)

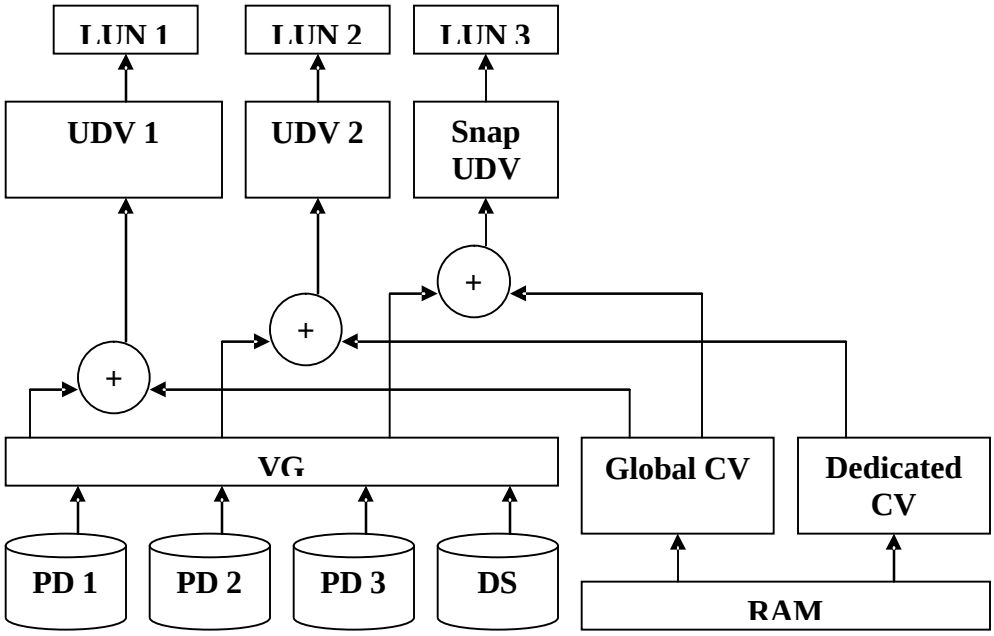
3.6 Volume configuration

Select **“Volume config”** to setup volume configurations including **“Physical disk”**, **“Volume group”**, **“User data volume”**, **“Cache volume”,** and **“Logical unit”** functions.

Physical disk	Hard disks to store data
Volume group	Sets of physical disks with RAID functions
User data volume	Slices of volume groups
Cache volume	Dedicated or global cache space for user data volume
Logical unit	Target volumes for hosts access

Figure 3.6.1

3.6.1 Volume relationship diagram



The above diagram describes the relationship of RAID components. One VG (Volume Group) consists of a set of UDVs (User Data Volume) and owns one RAID level attribute. Each VG can be divided into several UDVs. The UDVs from one VG share the same RAID level, but may have different volume capacity. Each UDV will be associated with one specific CV (Cache Volume) to execute the data transaction. Each CV could have different cache memory size from

user's modification/setting. LUN is the logical volume/unit, which the users could access through SCSI commands.

3.6.2 Physical disk

Enter **"Physical disk"** to view the status of hard drives inserted in the system. Below are operation tips:

1. Multiple select. Select one or more checkboxes in front of the slot number or select the checkbox at the top left corner, this will select all disk. Uncheck this box, this will deselect all.
2. The list box will disappear if there is no VG or only VG of RAID 0, JBOD are listed because these RAID levels cannot be set as dedicated spare disks.

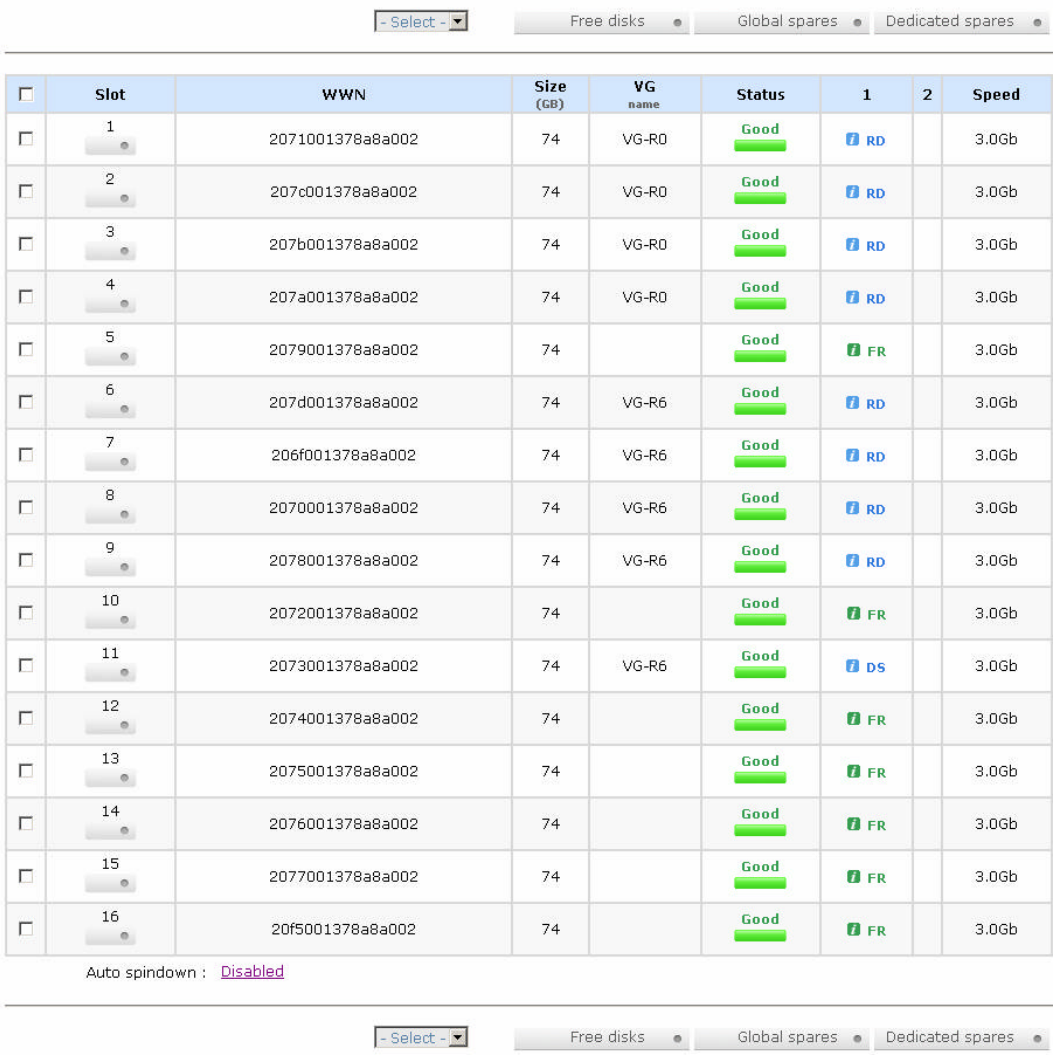

- Select -
Free disks
Global spares
Dedicated spares
Slot
WWN
Size (GB)
VG name
Status
1
2
Speed
1 2071001378a8a002 74 VG-R0 Good RD 3.0Gb
2 207c001378a8a002 74 VG-R0 Good RD 3.0Gb
3 207b001378a8a002 74 VG-R0 Good RD 3.0Gb
4 207a001378a8a002 74 VG-R0 Good RD 3.0Gb
5 2079001378a8a002 74 Good FR 3.0Gb
6 207d001378a8a002 74 VG-R6 Good RD 3.0Gb
7 206f001378a8a002 74 VG-R6 Good RD 3.0Gb
8 2070001378a8a002 74 VG-R6 Good RD 3.0Gb
9 2078001378a8a002 74 VG-R6 Good RD 3.0Gb
10 2072001378a8a002 74 Good FR 3.0Gb
11 2073001378a8a002 74 VG-R6 Good DS 3.0Gb
12 2074001378a8a002 74 Good FR 3.0Gb
13 2075001378a8a002 74 Good FR 3.0Gb
14 2076001378a8a002 74 Good FR 3.0Gb
15 2077001378a8a002 74 Good FR 3.0Gb
16 20f5001378a8a002 74 Good FR 3.0Gb
Auto spindown : Disabled
- Select -
Free disks
Global spares
Dedicated spares

Figure 3.6.2.1

(Figure 3.6.2.1: Physical disks of slot 1,2,3,4 are created for a VG named "VG-R0". Physical disks of slot 6,7,8,9 are created for a VG named "VG-R6". Slot 11 is set as dedicated spare disk of VG named "VG-R6". The others are free disks.)

- **PD column description:**

Slot	The position of the hard drives. The active button next to the slot number **"More Information"** will provide more details on the hard drive.
WWN	**W**orld **W**ide **N**ame.
Size (GB)	Capacity of hard drive.
VG Name	Related volume group name.
Status	The status of hard drive. **"GOOD"** à the hard drive is good. **"DEFECT"** à the hard drive has bad blocks. **"FAIL"** à the hard drive has failed.
Status 1	**"RD"** à **R**AID **D**isk. This hard drive has been set to RAID. **"FR"** à **FR**ee disk. This hard drive is free for use. **"DS"** à **D**edicated **S**pare. This hard drive has been set to be a dedicated spare of the VG. **"GS"** à **G**lobal **S**pare. This hard drive has been set to be a global spare of all VGs. **"RS"** à **R**e**S**erve. The hard drive contains the VG information but cannot be used. It may be caused by an uncompleted VG set, or hot-plugging the disk while there is drive activity. In order to protect the data in the disk, the status changes to reserve. It can be reused after setting it to "FR" manually.
Status 2	**"R"** à **R**ebuild. The hard drive is rebuilding. **"M"** à **M**igration. The hard drive is doing migration.

Speed	**3.0G** à From SATA ATAPI standard, the disk can support ATAPI IDENTIFY PACKET DEVICE command, and the speed can achieve Serial ATA Gen-2 signaling speed (3.0Gbps). **1.5G** à From SATA ATAPI standard, the disk can support ATAPI IDENTIFY PACKET DEVICE command, and the speed can achieve Serial ATA Gen-1 signaling speed (1.5Gbps). **Unknown** à The disk doesn't support above command, so the speed is defined as unknown.

- **PD operations description:**

Free disks	Make the selected hard drive to be free for use.
Global spares	Set the selected hard drive(s) as a global spare for all VGs.
Dedicated spares	Set hard drive(s) as a dedicated spare for a selected VGs.

In this page, IS8P2G also provides HDD auto spindown down function to save power. The default value is disabled.

Figure 3.6.2.2

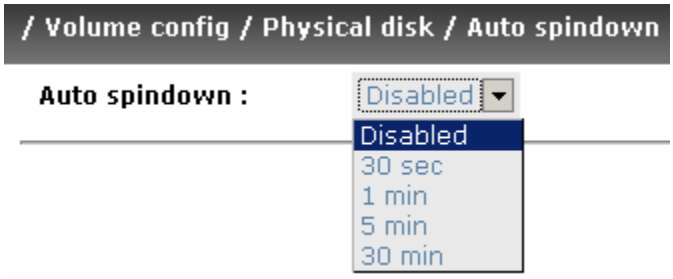


Figure 3.6.2.3

3.6.3 Volume Group

Select **“Volume group”** to view the status of each volume group.

- **VG column description:**

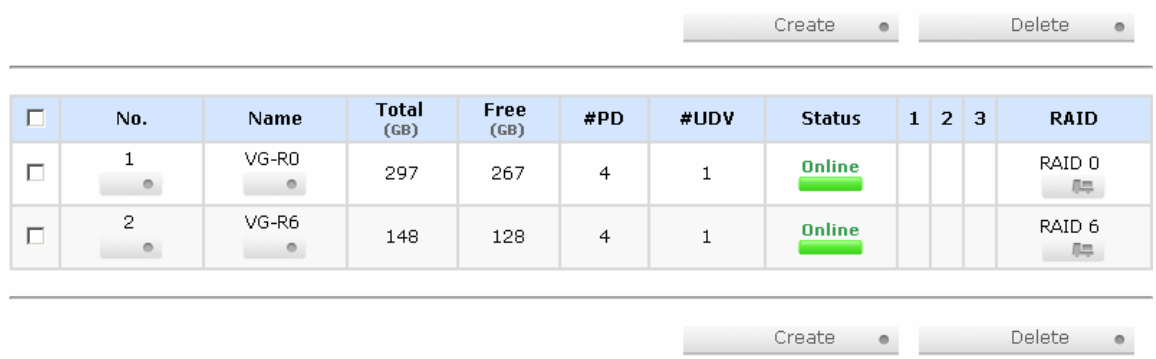


Figure 3.6.3.1

(Figure 3.6.3.1: There is a RAID 0 with 4 physical disks, named “VG-R0”, total size is 297GB, free size is 267GB, related to 1 UDV. Another is a RAID 6 with 4 physical disks, named “VG-R6”.)

No.	Number of the volume group. The active button next to the volume group **“More Information”** will provide more details on the volume group.
Name	Volume group name. The button next to the name is **“Rename”** function.
Total(GB)	Total capacity of this volume group.
Free(GB)	Free capacity of this volume group.
#PD	The number of physical disks of the volume group.
#UDV	The number of user data volumes related to the volume group.
Status	The status of volume group. **“Online”** à volume group is online. **“Fail”** à volume group failed.

Status 1	**“DG”** à **D**e**G**raded mode. This volume group is not complete. The reason could be a missing disk or failure of disk.
Status 2	**“R”** à **R**ebuild. This volume group is rebuilding.
Status 3	**“M”** à **M**igration. This volume group is migrating.
RAID	The RAID level of the volume group. The button next to the RAID level is **“Migrate”** function. Click **“Migrate”** to add disk(s) to do expansion or change the RAID level of the Volume group.

- **VG operations description:**

Create	Create a volume group
Delete	Delete a volume group

3.6.4 User Data Volume

Enter **“User data volume”** function to view the status of each user data volume.

Figure 3.6.4.1

(Figure 3.6.4.1: Create a UDV named “QUICK41473”, related to “QUICK17810”, size is 519GB, status is online, write back, high priority, related to 1 LUN, with cache volume 878MB.)

- **UDV column description:**

No.	Number of this user data volume. The button below the UDV No. is **"More Information"**. It shows the details of the User Data Volume.
Name	Name of this user data volume. The button below the UDV Name is **"Rename"** function.
Size(GB)	Total capacity of this user data volume. The button below the size is **"Extend"** function.
Status	The status of this user data volume. **"Online"** à user data volume is online. **"Fail"** à user data volume failed.
Status 1	**"WT"** à **W**rite **T**hrough. **"WB"** à **W**rite **B**ack. **"RO"** à **R**ead **O**nly. The button below the status1 is **"Set read/write mode"** function.
Status 2	**"HI"** à **HI**gh priority. **"MD"** à **M**i**D** priority. **"LO"** à **LO**w priority. The button below the status2 is **"Set Priority"** function.
Status 3	**"I"** à user data volume is initializing. **"R"** à user data volume is rebuilding. **"M"** à user data volume is migrating.
R %	Ratio of initializing or rebuilding.
RAID	The RAID level the user data volume is using.
#LUN	Number of LUN(s) the data volume is attached to.
VG name	The VG name of the user data volume.
CV (MB)	The cache volume of the user data volume.

- **UDV operations description:**

Attach	Attach to a LUN.
Create	Create a user data volume function.
Delete	Delete a user data volume function.

3.6.5 Cache volume

Select **“Cache volume”** function to view the status of cache volume.

The global cache volume is the default cache volume, which is created after turning the power on of the ISC8P2G and it cannot be deleted. The size of global cache is based on the RAM size. It is the total memory size minus the system usage.

Figure 3.6.5.1

- **CV column description:**

No.	Number of the Cache volume. The button next to the CV No. is **“More Information”.** It shows the details of the cache volume.
Size(MB)	Total capacity of the cache volume The button next to the CV size is **“Resize”** function. The CV size can be adjusted.
UDV Name	Name of the UDV.

- **CV operations description:**

Create	Create a cache volume function.
Delete	Delete a cache volume function.

If there is no free space for creating a new dedicated cache volume, decrease the global cache size first. After modifying the size, the dedicated cache volume can be created.

Tips
The minimum size of global cache volume is **40MB**. The minimum size of dedicated cache volume is **20MB**.

3.6.6 Logical unit number

Select **"Logical unit"** function to view the status of the attached logical unit number of each UDV.

User can attach LUN by clicking the "Attach". Please refer to Figure 3.6.6.1.

For the **"Host"** parameter, you can input an initiator node name for access control, or fill-in wildcard **"*",** which means every host can access the volume.
Choose LUN number and permission, then click "Confirm". Please refer to Figure 3.6.6.2.

You can assign up to 256 LUNs per system (ISC8P2G). For the host connection, the host number limitation is 32 per system (ISC8P2G). To access a single user data volume (UDV) simultaneously, the host number limitation is 8, which means 8 hosts can access the same UDV at the same time.

Figure 3.6.6.1

(Figure 3.6.6.1: (Single-node).

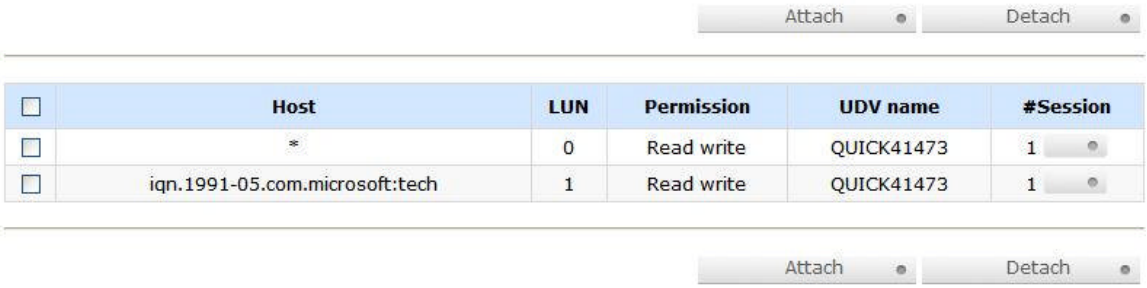


Figure 3.6.6.2

(Figure 3.6.6.2: ISC8P2G, QUICK41473 is attached to LUN 0 where every host can access. QUICK41473 is attached to LUN 1 with only initiator named "iqn.1991-05.com.microsoft:tech" can access.)

- **LUN operations description:**

Attach	Attach a logical unit number to a user data volume.
Detach	Detach a logical unit number from a user data volume.

The matching rules of access control are from top to bottom by sequence. For example, if there are 2 rules for the same UDV, one is "*", LUN 0; the other is "iqn.host1", LUN 1. The other host "iqn.host2" can login because it matches the rule 1.

The access will be denied when there is no matching rule.

3.6.7 Examples

The following are examples for creating volumes. Example 1 shows how to create two UDVs sharing the same CV (global cache volume) and set a global spare disk. Example 2 shows how to create two UDVs. One shares global cache volume, the other uses dedicated cache volume and set a dedicated spare disk.

- **Example 1**

Example 1 shows how to create two UDVs in one VG, each UDV uses global cache volume. Global cache volume is created automatically after the system boots up. So, no action is needed to set CV. You can then set a global spare disk. The example also shows a procedure on how to delete the UDV.

Step 1: Create VG (Volume Group).

To create the volume group, please follow the procedures below:

Figure 3.6.7.1

1. Select **"/ Volume config / Volume group"**.
2. Click " Create ".
3. Input a VG Name, choose a RAID level from the picklist, press " Select PD " to choose the RAID PD slot(s), then press " Next >> ".
4. Check the results. Press " Confirm " if all setups are correct.
5. Done. A VG has been created.

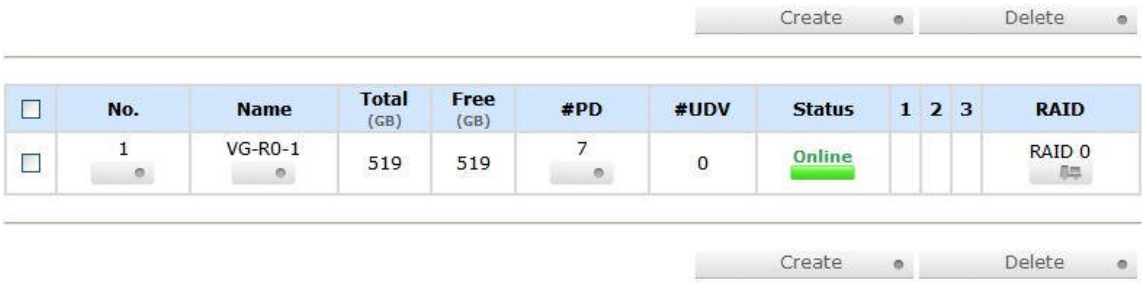


Figure 3.6.7.2

(Figure 3.6.7.2: Creating a RAID 0 with 7 physical disks, named "VG-R0-1". The total size is 519GB. Because no UDV are created, free size still remains 519GB.)

Step 2: Create UDV (User Data Volume).

To create a data user volume, please follow the procedures.

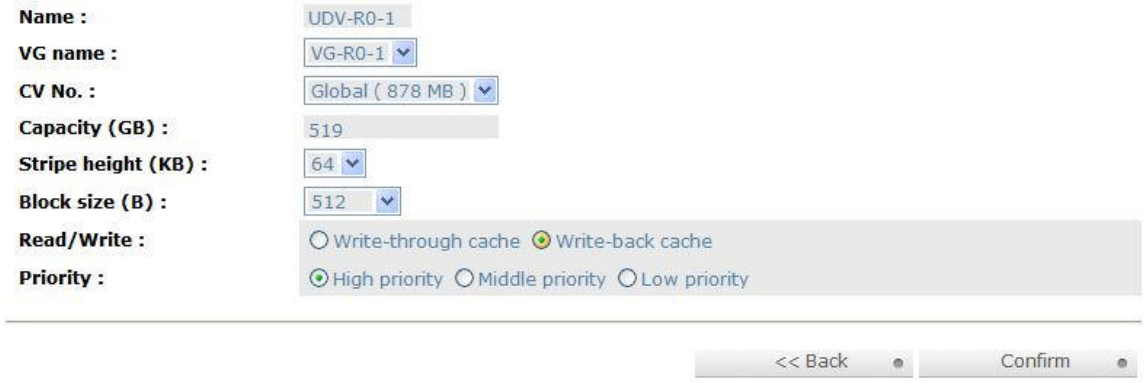


Figure 3.6.7.3

1. Select **"/ Volume config / User data volume"**.
2. Click "Create".
3. Input a UDV name, choose a VG Name and input a size to the UDV. Decide the stripe height, block size, read/write mode and set priority. Finally click "Confirm".
4. Done. A UDV has been created.
5. Create another UDV.

Figure 3.6.7.4

(Figure 3.6.7.4: Create UDVs named "UDV-R0-1" and "UDV-R0-2", related to "VG-R0-1", the size of "UDV-R0-1" is 300 GB, the size of "UDV-R0-2" is 219GB. The status of these UDVs are online, write back, high priority with cache volume 878MB. There is no LUN attached.)

Step 3: Attach LUN to UDV.

There are 2 methods to attach LUN to UDV.

1. In **"/ Volume config / User data volume"**, press "Attach".
2. In **"/ Volume config / Logical unit"**, press "Attach".

The procedures are as follows:

Figure 3.6.7.5

1. Select a UDV.
2. Input **"Host"**, which can be an initiator node name for access control, or fill-in wildcard **"*",** which means every host can access this volume. Choose LUN and permission, then click "Confirm".
3. Done.

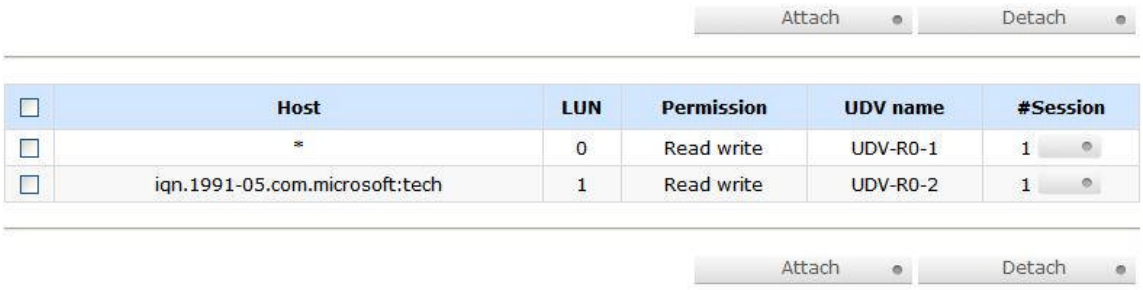


Figure 3.6.7.6

(Figure 3.6.7.6: UDV-R0-1 is attached to LUN 0 with any hosts can access. UDV-R0-2 is also attached to LUN 1 with only initiator named "iqn.1991-05.com.microsoft:tech" can access.)

Tips
The matching rules of access control are from top to bottom by sequence. Please refer 3.6.6 for details.

Step 4: Set global spare disk.

To set global spare disks, please follow the steps below.

1. Select **"/ Volume config / Physical disk"**.
2. Select the free disk(s) by clicking the checkbox, then click " Global spares " to set as global spares.
3. There is a "GS" icon shown up at status 1 column.

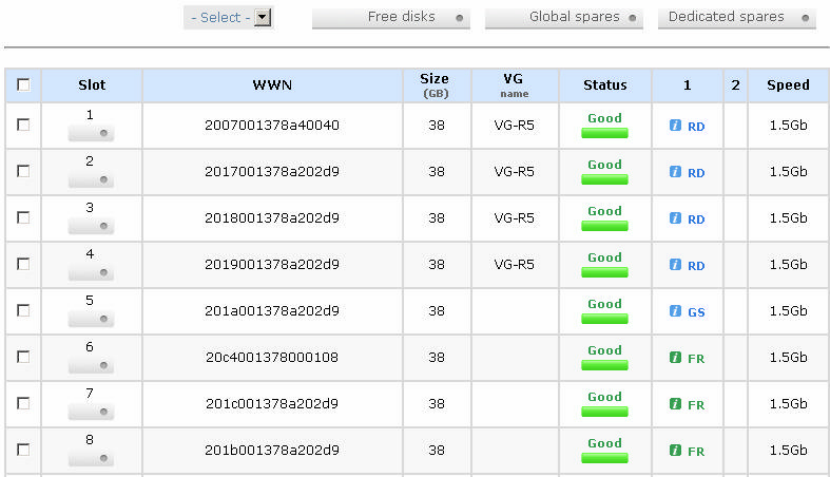


Figure 3.6.7.7

(Figure 3.6.7.7: Slot 5 is set as global spare disk.)

Step 5: Done. They can be used as iSCSI disks.
To delete UDVs and VG, please follow the steps.

Step 6: Detach LUN from UDV.

In **"/ Volume config / Logical unit"**,

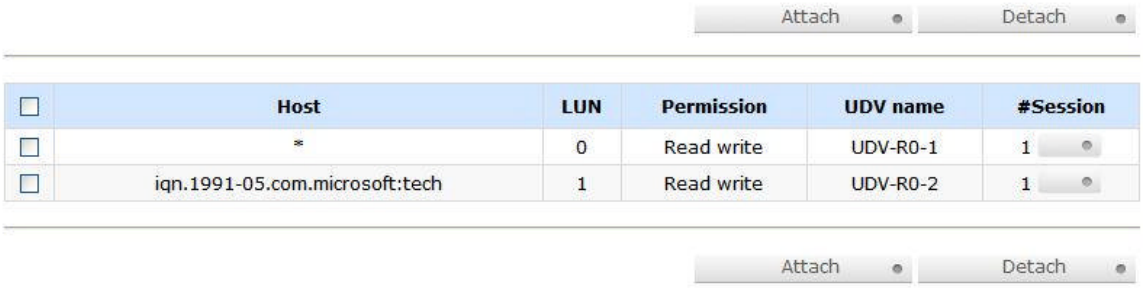


Figure 3.6.7.8

1. Select LUNs by clicking the checkbox, then click "Detach". A confirmation page will open up.
2. Choose "OK".
3. Done.

Step 7: Delete UDV (User Data Volume).

To delete the user data volume, please follow the steps below:

1. Select **"/ Volume config / User data volume"**.
2. Select UDVs by clicking the checkbox.
3. Click "Delete". A confirmation page will open up.
4. Choose "OK".
5. Done. The UDVs are deleted.

Tips
When deleting UDV, the attached LUN(s) related to this UDV will be detached automatically, too.

Step 8: Delete VG (Volume Group).

To delete the volume group, please follow the steps below:

1. Select **"/ Volume config / Volume group"**.
2. Select a VG by clicking the checkbox, make sure that there is no UDV on this VG, or the UDV(s) on this VG must be deleted first.
3. Click " ". A confirmation page will open up.
4. Choose "OK"
5. Done. The VG has been deleted.

Tips
The action of deleting one VG will succeed only when all of the related UDV(s) are deleted in this VG. Otherwise, you will get an error when deleting this VG.

Step 9: Free global spare disk.

To free global spare disks, please follow the procedures.

1. Select **"/ Volume config / Physical disk"**.
2. Select the global spare disk by clicking the checkbox of the row, then click " " to free disk.

Step 10: Done, all volumes have been deleted.

- **Example 2**

Example 2 shows how to create two UDVs in one VG. One UDV shares global cache volume, the other uses dedicated cache volume. First, the dedicated cache volume should be created. It can be used in creating UDV. A procedure also shows how to delete the UDV.

Each UDV is associated with one specific CV (cache volume) to execute the data transaction. Each CV could have different cache memory size. If there is no special request in the UDVs, it uses global cache volume. You can also create a dedicated cache for individual UDV manually. Using dedicated cache volume, the performance would not be affected by the other UDV's data access.

The total cache size depends on the RAM size and it is set automatically as the global cache. To create a dedicated cache volume, the first step is to decrease the global cache size for the dedicated cache volume. Please follow the steps below.

Step 1: Create dedicated cache volume.

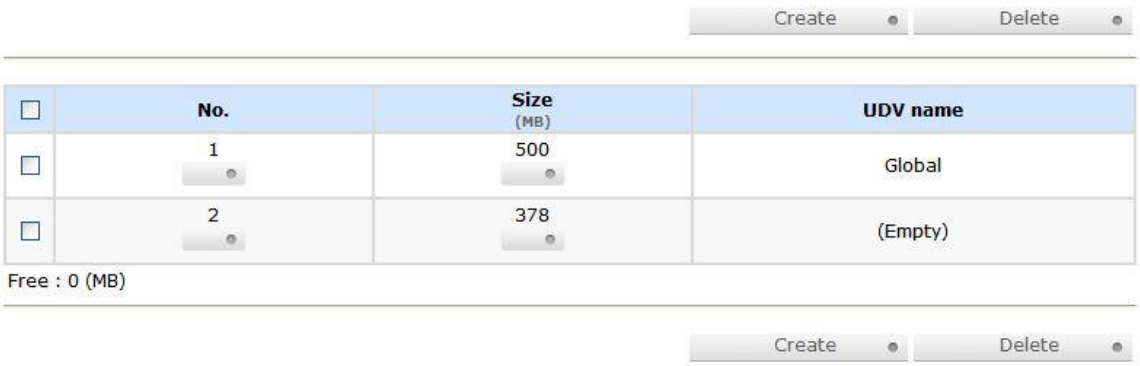


Figure 3.6.7.9

1. Select **"/ Volume config / Cache volume"**.
2. If there is no free space for creating a new dedicated cache volume, decrease the global cache size first by clicking the button " " in the size column. After modifying size, click " Confirm " to return to cache volume page.
3. Click " Create " to enter the setup page.
4. Fill in the size and click " Confirm ".
5. Done. A new dedicated cache volume has been set.

Tips
The minimum size of global cache volume is **40MB**. The minimum size of dedicated cache volume is **20MB**.

Step 2: Create VG (Volume Group).

Please refer to Step 1 of Example 1 to create VG.

Step 3: Create UDV (User Data Volume).

Please refer to Step 2 of Example 1 to create UDV. To create a data user volume with dedicated cache volume, please follow the steps below.

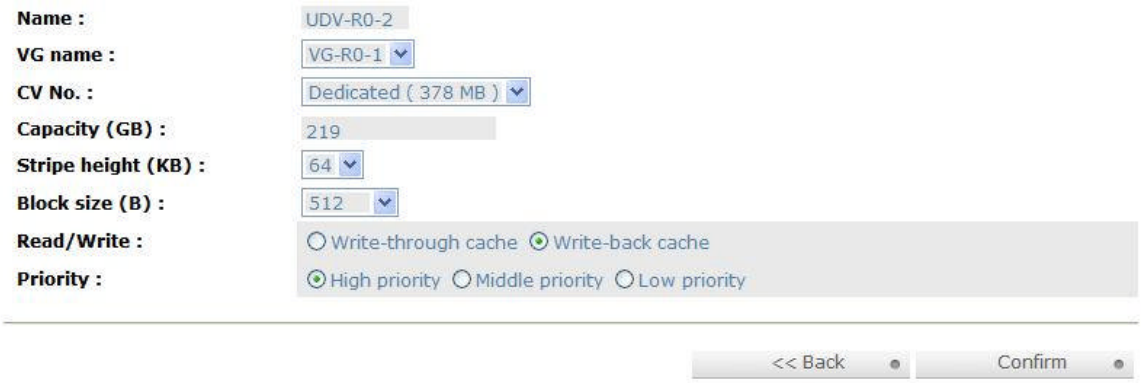


Figure 3.6.7.10

1. Select **"/ Volume config / User data volume"**.
2. Click "Create".
3. Input a UDV name, choose a VG Name, select **Dedicated** cache which is created at Step 1, and input the size for the UDV. Decide the stripe height, block size, read/write mode and set priority, finally click "Confirm".
4. Done. A UDV using dedicated cache has been created.

Figure 3.6.7.11

(Figure 3.6.7.11: UDV named "UDV-R0-1" uses global cache volume 500MB, and "UDV-R0-2" uses dedicated cache volume 378MB.)

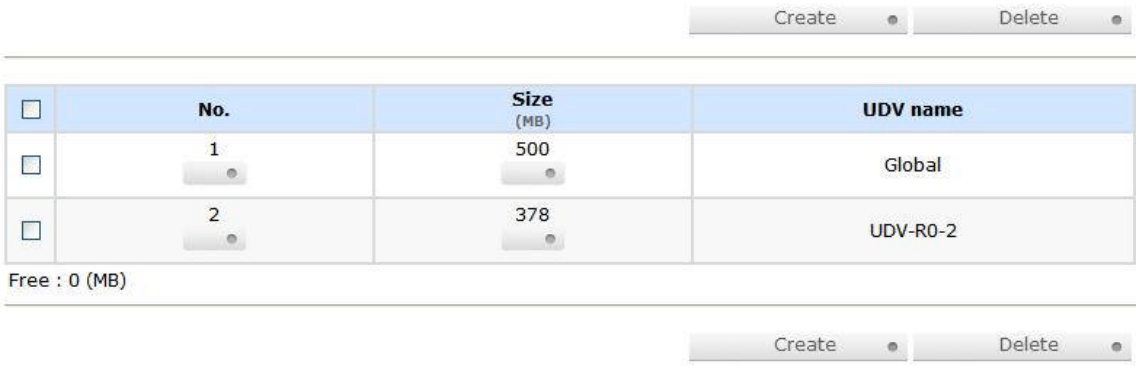


Figure 3.6.7.12

(Figure 3.6.7.12: In "/ Volume config / Cache volume", UDV named "UDV-R0-2" uses dedicated cache volume 378MB.)

Step 4: Attach LUN to UDV.

Please refer to Step 3 of Example 1 to attach LUN.

Step 5: Set dedicated spare disk.

To set dedicated spare disks, please follow the steps below:

1. Select **"/ Volume config / Physical disk"**.
2. Select a VG from the list box, then select the free disk(s), click " Dedicated spares " to set as dedicated spare for the selected VG.
3. There is a "DS" icon shown up at status 1 column.

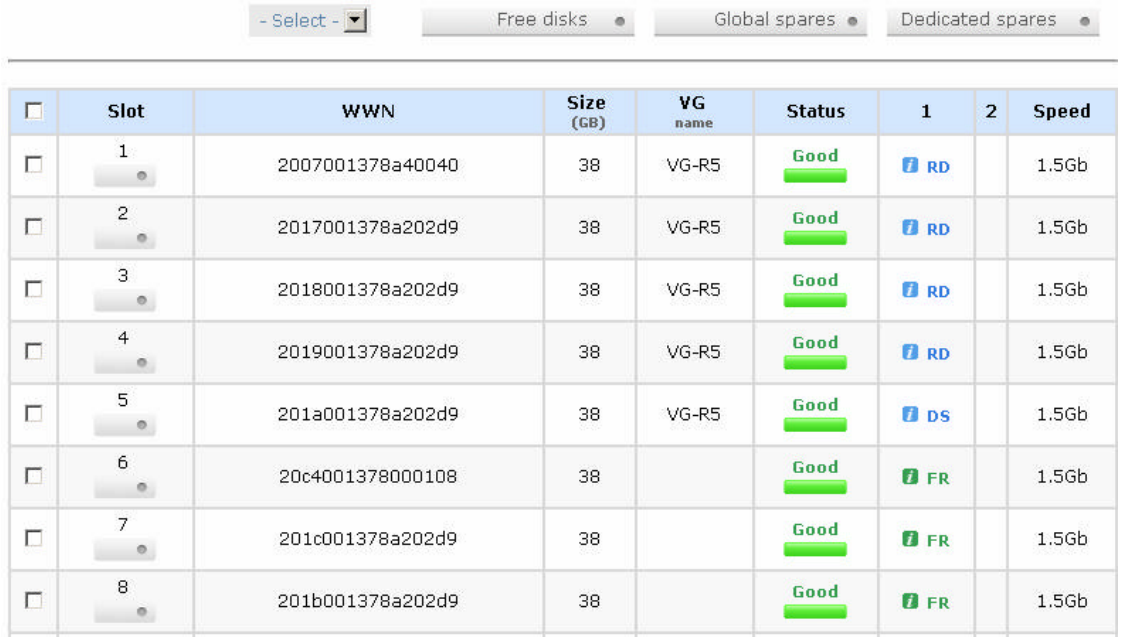


Figure 3.6.7.13

(Figure 3.6.7.13: Slot 5 has been set as dedicated spare disk of VG named "VG-R5".)

Step 6: Done. The PDs can be used as iSCSI disks.

To delete UDVs, VG, please follow the steps.

Step 7: Detach LUN from UDV.

Please refer to Step 6 of Example 1 to detach LUN.

Step 8: Delete UDV (User Data Volume).

Please refer to Step 7 of Example 1 to delete UDV.

Step 9: Delete VG (User Data Volume).

Please refer to Step 8 of Example 1 to delete VG.

Step 10: Free dedicated spare disk.

To free dedicated spare disks, please follow the steps below:

1. Select **"/ Volume config / Physical disk"**.
2. Select the dedicated spare disk by clicking the checkbox, then click "

" to free disk.

Step 11: Delete dedicated cache volume.

To delete the cache volume, please follow the steps below:

1. Select **"/ Volume config / Cache volume"**.
2. Select a CV by clicking the checkbox.
3. Click "

". A confirmation page will open up.
4. Choose "OK".
5. Done. The CV has been deleted.

Caution
Global cache volume cannot be deleted.

Step 12: Done. All volumes have been deleted.

3.7 Enclosure management

The **“Enclosure management”** function allows managing the enclosure information including **“SES config”**, **“Hardware monitor”**, **“S.M.A.R.T.”** and **“UPS”**. The enclosure management provides sensors for different purposes, such as temperature sensors, voltage sensors, hard disks, fan sensors, power sensors, and LED status. And because the hardware characteristics are different among these sensors, different sensors have different polling intervals. Below are the details for the polling time intervals:

1. Temperature sensors: 1 minute.
2. Voltage sensors: 1 minute.
3. Hard disk sensors: 10 minutes.
4. Fan sensors: 10 seconds, when there are continuous 3 times of error, ISC8P2G sends ERROR event log.
5. Power sensors: 10 seconds, when there are continuous 3 times of error, ISC8P2G sends ERROR event log.
6. LED status: 10 seconds.

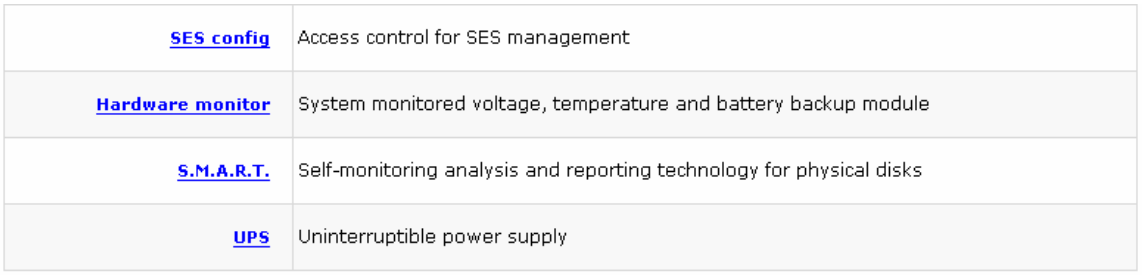


Figure 3.7.1

3.7.1 SES configuration

SES represents **S**CSI **E**nclosure **S**ervices, one of the enclosure management standards. The **“SES config”** function allows you to enable or disable the management of SES.

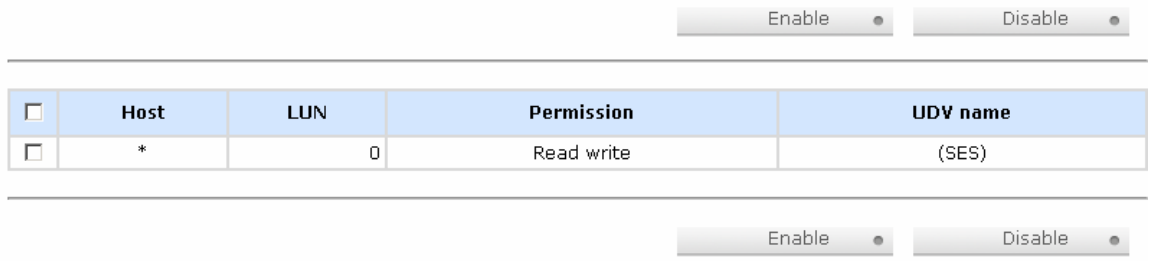


Figure 3.7.1.1

(Figure 3.7.1.1: Enable SES in LUN 0, and can be accessed from every host.)

The SES client software is available at the following web site:
SANtools: http://www.santools.com/

3.7.2 Hardware monitor

Select **"Hardware monitor"** function to view information on current voltage and temperature.

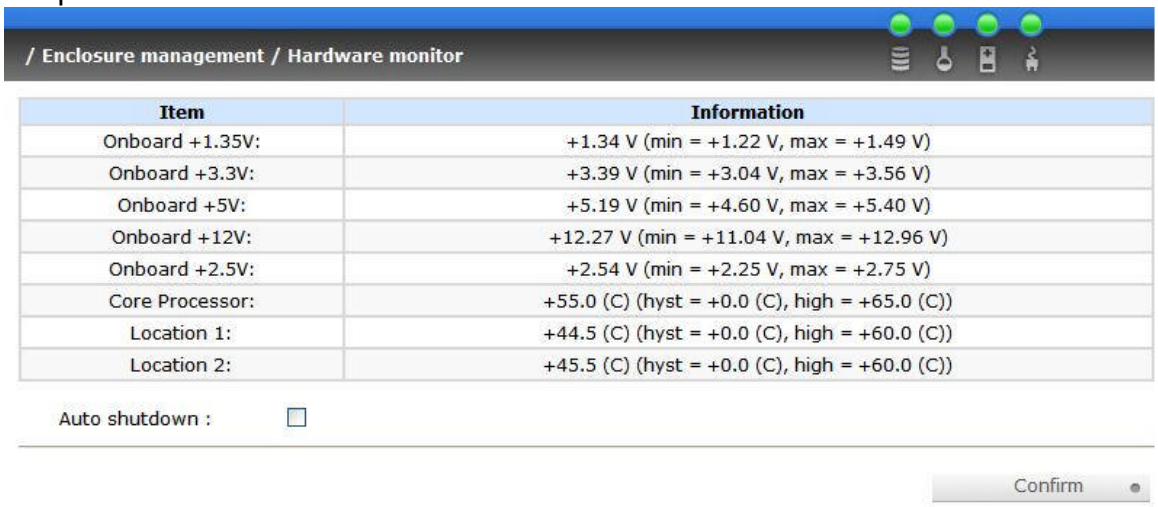

/ Enclosure management / Hardware monitor
Item
Information
Onboard +1.35V:
+1.34 V (min = +1.22 V, max = +1.49 V)
Onboard +3.3V:
+3.39 V (min = +3.04 V, max = +3.56 V)
Onboard +5V:
+5.19 V (min = +4.60 V, max = +5.40 V)
Onboard +12V:
+12.27 V (min = +11.04 V, max = +12.96 V)
Onboard +2.5V:
+2.54 V (min = +2.25 V, max = +2.75 V)
Core Processor:
+55.0 (C) (hyst = +0.0 (C), high = +65.0 (C))
Location 1:
+44.5 (C) (hyst = +0.0 (C), high = +60.0 (C))
Location 2:
+45.5 (C) (hyst = +0.0 (C), high = +60.0 (C))
Auto shutdown :
Confirm

Figure 3.7.2.1

If **"Auto shutdown"** has been checked, the system will shutdown automatically when voltage or temperature is out of the normal range. For better data protection, please check "**Auto Shutdown**".

For better protection and to avoid single short period of high temperature triggering Auto shutdown, ISC8P2G use multiple condition judgments for Auto shutdown. Below are the details of when the Auto shutdown will be triggered.

1. There are 3 sensors placed on the ISC8P2G for temperature checking of the core processor, on the PCI-X bridge, and on the daughter board. ISC8P2G will check each sensor every 30 seconds. When one of the sensor senses high temperature value for 3 minutes, the Auto shutdown will be triggered immediately.
2. The core processor temperature limit is 85 Ž. The PCI-X bridge temperature limit is 80 Ž. The daughter board temperature limit is 80 Ž.
3. If the high temperature situation doesn't last for 3 minutes, ISC8P2G will not do auto shutdown.

3.7.3 Hard drive S.M.A.R.T. function support

S.M.A.R.T. (**S**elf-**M**onitoring **A**nalysis and **R**eporting **T**echnology) is a diagnostic tool for hard drives to give advanced warning of drive failures. **S.M.A.R.T.** provides users a chance to take actions before possible drive failure.

S.M.A.R.T. measures many attributes of the hard drive all the time and determine if the hard drives which are close to failure. The advanced notice of possible hard drive failure can allow users to back up hard drive or replace the hard drive. This is much better than hard drive crash when it is writing data or rebuilding a failed hard drive.

The **"S.M.A.R.T."** function will display S.M.A.R.T. information of hard drives. The number value is the current value and the number in parenthesis is the threshold value. The threshold values of hard drive vendors are different; please refer to vendors' specification for details.

S.M.A.R.T. information is only supported on SATA drive. SAS drive does not have S.M.A.R.T. information. It will show N/A in this web page.

Slot	Read error rate	Spin up time	Reallocated sector count	Seek error rate	Spin up retries	Calibration retries	Temperature (C)
1	200(51)	187(21)	200(140)	200(51)	100(51)	100(51)	27
2	200(51)	167(21)	200(140)	200(51)	100(51)	100(51)	29
3	200(51)	159(21)	200(140)	200(51)	100(51)	100(51)	30
4	200(51)	167(21)	200(140)	200(51)	100(51)	100(51)	34
5	200(51)	163(21)	200(140)	200(51)	100(51)	100(51)	30
6	100(16)	103(24)	100(5)	100(67)	100(60)	N/A	34
7	200(51)	161(21)	200(140)	200(0)	100(0)	100(0)	31

Figure 3.7.3.1

3.7.4 UPS

Select **“UPS”** function. It will set UPS (**U**ninterruptible **P**ower **S**upply) parameters.

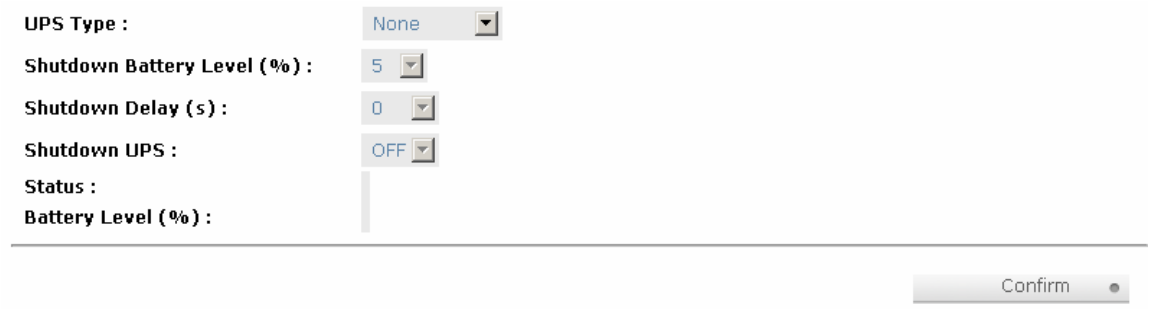


Figure 3.7.4.1

Currently, the system only supports and communicates with smart-UPS function of APC (American Power Conversion Corp.) UPS. Please check detail from http://www.apc.com/.

First, connect the system and APC UPS via RS-232. Then set up the shutdown value.

UPS Type	Select UPS Type. Choose Smart-UPS for APC. None for other vendors or no UPS.
Shutdown Battery Level (%)	When value is below the setting level, the system will shutdown. Setting level to **“0”** will disable UPS function.
Shutdown Delay (s)	If power failure has occurred, and the system cannot return to the set value on the set period, the system will shutdown. Setting delay to **“0”** will disable the function.
Shutdown UPS	Select ON. When power on the UPS is almost depleted, the UPS will shutdown by itself after the ISC8P2G shutdown successfully. After power comes back on, the UPS will start working and notify system to boot up. Selecting OFF will not turn off the UPS automatically.

Status	The status of UPS. **“Detecting…”** **“Running”** **“Unable to detect UPS”** **“Communication lost”** **“UPS reboot in progress”** **“UPS shutdown in progress”** **“Batteries failed. Please change them NOW!”**
Battery Level (%)	Current percentage of battery level.

3.8 System Maintenance

“Maintenance” function allows operation of the system functions including “**Upgrade”** to the latest firmware, **“Info”** to show the system version, “**Reset to default**” to reset all ISC8P2G configuration values to origin settings, “**Config import & export**” to export and import all controller configuration except for VG/UDV setting and LUN setting, and **“Shutdown”** to either reboot or shutdown the system.

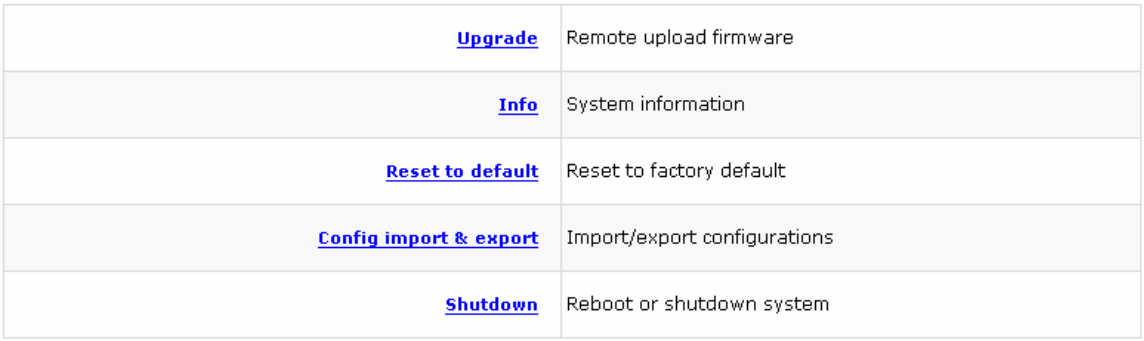


Figure 3.8.1

3.8.1 Upgrade

Select **“Upgrade”** function to upgrade firmware. Please prepare new firmware file named **“xxxx.bin”** in local hard drive, then press “ Browse... ” to select the file. Click “ Confirm ”, it will open a message “Upgrade system now?

If you plan to downgrade to the previous firmware later on, please export your system config first”, click **“Cancel”** to export system config, then click **“OK”** to start the upgrade.

Figure 3.8.1.1

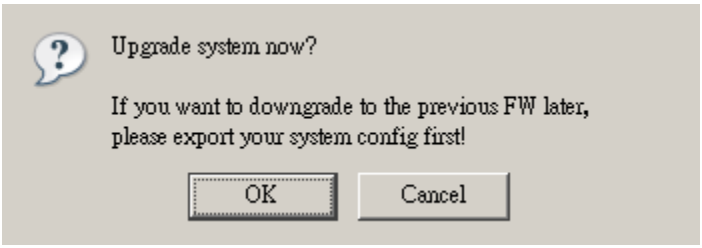


Figure 3.8.1.2

When upgrading, a progress bar will be seen running. After the upgrade, the system must be manually rebooted.

3.8.2 Info

“Info” function will display system information (including firmware version), CPU type, installed system memory, and controller serial number.

3.8.3 Reset to default

“Reset to default” function allows user to reset ISC8P2G to the factory default setting.

Figure 3.8.3.1

Reset to default sets password to default: **supervisor**, and set IP address to default as DHCP setting.

Default IP address: **192.168.0.1 (DHCP)**

Default subnet mask: **255.255.255.0**

Default gateway: **192.168.0.254**

3.8.4 Config import & export

“Config import & export” function allows user to save system configurable values like export function, and to apply all import function configuration. For the volume config setting, the values are available in export function but not available in import function to avoid conflict/date-deleting between two ISC8P2G.

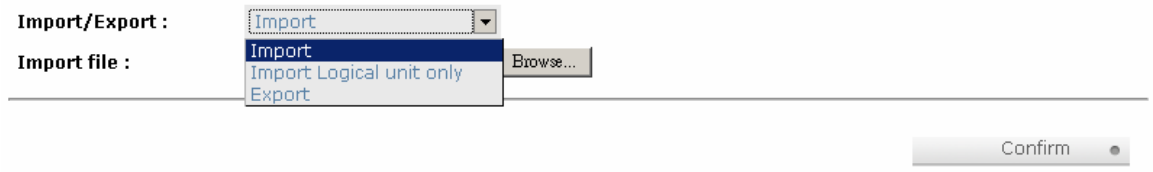


Figure 3.8.4.1

1. **Import:** Import all system configurations excluding volume config.
2. **Import Logical unit only:** No system and volume configurations, import LUN configurations only.
3. **Export:** Export all configurations to a file.

Caution
Import function will import all system configurations excluding volume config.

3.8.5 Shutdown

“Shutdown” function will display **“Reboot”** and **“Shutdown”** buttons. Before powering off, it’s better to press “Shutdown” to flush the data from cache to the physical disks. This step is recommended for the data protection.

Figure 3.8.5.1

3.9 Logout

For security reason, **“Logout”** function will allow logout while no user is operating the ISC8P2G. To log back in, enter username and password again.

Chapter 4 Advanced operation

4.1 Rebuild

If one of the physical disk on the VG which was set to a protected RAID level (e.g.: RAID 3, RAID 5, or RAID 6) has FAILED or has been unplugged/removed, then, the VG status is changed to degraded mode. The system will search/detect for a spare disk to **rebuild** the degraded VG. It will look for a dedicated spare disk first and if none is found, it will check if a global spare disk has been set up and use this disk for rebuild.

ISC8P2G supports Auto-Rebuild function. If the RAID level set on the VG is protected, such as RAID 3, RAID 5, RAID 6, and etc, ISC8P2G starts Auto-Rebuild as shown on the scenario below:

Take RAID 6 for example:

1. When there is no global spare disk or dedicated spare disk on the system, ISC8P2G will be in degraded mode and wait until (A) there is one disk assigned as spare disk, or (B) the failed disk is removed and replaced with new clean disk, then the Auto-Rebuild starts. The new disk will be a spare disk to the original VG automatically.

a. If the new added disk is not clean (with data on it), it would be marked as RS (reserved) and the system will not start "auto-rebuild".

b. If this disk does not belong to any existing VG, it would be FR (Free) disk and the system will start Auto-Rebuild function.

c. If user only removes the failed disk and plugs the same failed disk in the same slot again, the auto-rebuild will start. But rebuilding the array using the same failed disk may impact customer data later because of the unstable disk status. We suggest all customers not to rebuild the array using the same failed disk for better data protection.

2. When there is enough global spare disk(s) or dedicated spare disk(s) for the degraded array, ISC8P2G starts Auto-Rebuild immediately. And in RAID 6, if there is another disk failure happening during the time of rebuilding, ISC8P2G will start the above Auto-Rebuild scenario as well. And the Auto-Rebuild feature only works at "RUNTIME". It will not work during downtime. Thus, it will not conflict with the “Roaming” function.

In degraded mode, the status of VG is **“DG”**.

When rebuilding, the status of PD/VG/UDV is **“R”**; and **“R%”** in UDV will display the ratio in percentage. After complete rebuilding, **“R”** and **“DG”** will disappear.

Tips
The list box doesn’t exist if there is no VG or only VG of RAID 0, JBOD. This is because user cannot set dedicated spare disk for these RAID levels.

Sometimes, rebuild is called recover. These two have the same meaning. The table below lists the relationship between RAID levels and rebuild.

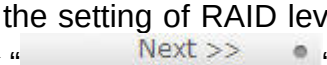
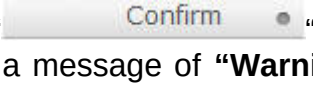
RAID 0	Disk striping. No protection of data. VG fails if any hard drive fails or gets unplug.
RAID 1	Disk mirroring over 2 disks. RAID 1 allows one hard drive failure or unplugging. Need one new hard drive to insert to the system for rebuild to be completed.
N-way mirror	Extension to RAID 1 level. It has N copies of the disk. N-way mirror allows N-1 hard drive failures or unplugging.
RAID 3	Striping with parity on the dedicated disk. RAID 3 allows one hard drive failure or unplugging.
RAID 5	Striping with interspersed parity over the member disks. RAID 5 allows one hard drive failure or unplugging.
RAID 6	2-dimensional parity protection over the member disks. RAID 6 allows two hard drive failure or unplugging. If it needs to rebuild two hard drives at the same time, it will rebuild the first one, then the other.
RAID 0+1	Mirroring of the members of the RAID 0 volumes. RAID 0+1 allows two hard drives to fail or gets unplugged, but they need to be part of the same array.
RAID 10	Striping over the members of the RAID 1 volumes. RAID 10 allows two hard drives to fail or gets unplugged, but they need to be part of different arrays.

RAID 30	Striping over the members of the RAID 3 volumes. RAID 30 allows two hard drives to fail or gets unplugged, but they need to be part of different arrays.
RAID 50	Striping over the member RAID 5 volumes. RAID 50 allows two hard drives to fail or gets unplugged, but they need to be part of different arrays.
RAID 60	Striping over the member RAID 6 volumes. RAID 40 allows four hard drives to fail or gets unplugged, but each two need to be part of different arrays.
JBOD	The abbreviation of **"J**ust a **B**unch **O**f **D**isks**"**. No protection of data. VG fails if any hard drive fails or gets unplug.

4.2 VG migration and expansion

To migrate the RAID level, follow the procedure below.

Note: If the VG migrates to the same RAID level of the original VG, it is expansion not migration.

1. Select **"/ Volume config / Volume group"**.
2. Decide which VG to be migrated, click the button " " in the RAID column next the RAID level.
3. Change the RAID level by clicking the down arrow " ". There will be a pop-up which shows if the HDD capacity is not enough to support the new setting RAID level, click " " to increase hard drives, then click " " to go back to setup page. When doing migration to a lower RAID level, such as the original RAID level is RAID 6 and user wants to migrate to RAID 0, the ISC8P2G will evaluate this operation if it is safe or not, and will display **"Sure to migrate to a lower protection array?"** to provide user warning.
4. Double check the setting of RAID level and RAID PD slot. If no issues are seen, click "  ".
5. Finally a confirmation page shows the detailed RAID info. If no problem arises, click "  " to start migration. The ISC8P2G also pops up a message of **"Warning: power lost during migration may cause damage of data!"** to provide user warning. When the power is turned off during migration, the data is in high risk.

6. Migration starts and it can be seen from the “status 3” of a VG with a running square and an **“M”**. In **“/ Volume config / User data volume”**, it displays an **“M”** in **“Status 4”** and complete percentage of migration in **“R%”**.

Figure 4.2.1

Figure 4.2.2

(Figure 4.2.2: A RAID 0 with 2 physical disks migrates to RAID 5 with 3 physical disks.)

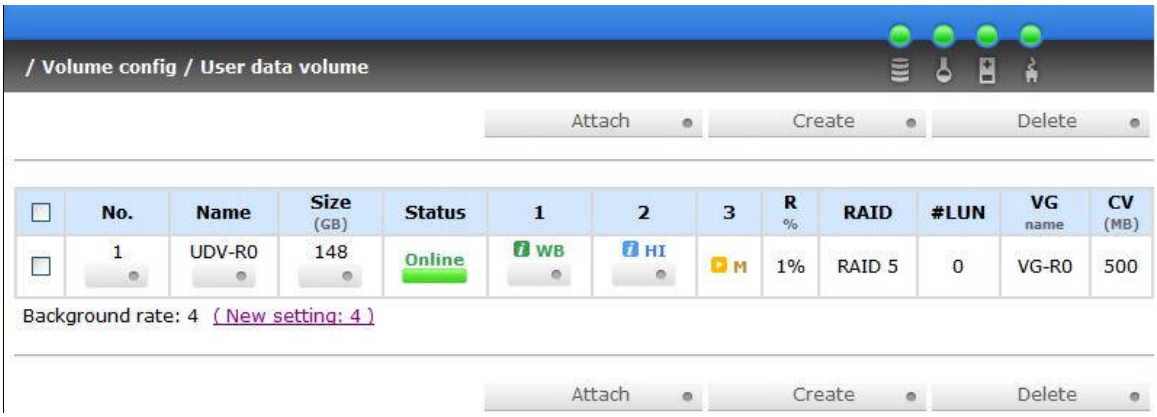


Figure 4.2.3

(Figure 4.2.3: A RAID 0 migrates to RAID 5, complete percentage is 1%.)

To do migration/expansion, the total size of VG must be larger or equal to the original VG. It does not allow expanding the same RAID level with the same hard disks of original VG.

When setting migration parameters, if a user does incorrect setup, the ISC8P2G will pop up warning messages. Below is the detail of messages.

1. **Invalid VG ID:** Source VG is invalid.
2. **Degrade VG not allowed:** Source VG is degraded.
3. **Initializing/rebuilding operation's going:** Source VG is initializing or rebuilding.
4. **Migration operation's going:** Source VG is already in migration mode.
5. **Invalid VG raidcell parameter:** Invalid configuration. E.g., New VG's capacity < Old VG's capacity, New VG's stripe size < Old VG's stripe size. Or New VG's configuration == Old VG's configuration.
6. **Invalid PD capacity:** New VG's minimum PD capacity < Old VG's minimum PD capacity.

Caution
VG Migration cannot be executed during rebuild or UDV extension.

4.3 UDV Extension

To extend UDV size, please follow the steps below.

1. Select **"/ Volume config / User data volume"**.
2. Decide which UDV to be extended. Click the button " " in the Size column next the number.
3. Change the size. The size must be larger than the original, and then click " Confirm " to start.
4. Extension starts. If UDV needs initialization, it will display an **"I"** in **"Status 3"** and complete percentage of initialization in **"R%"**.

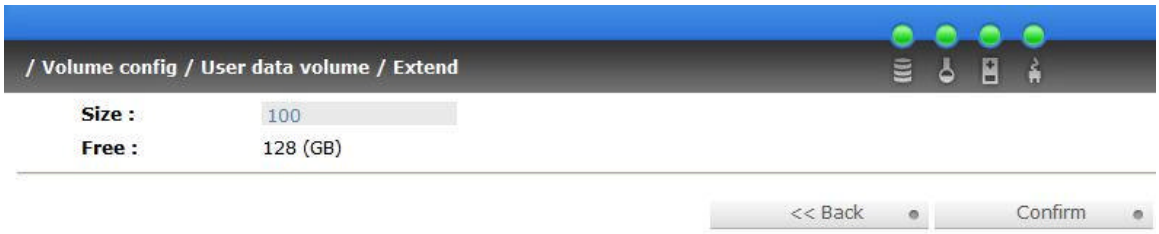


Figure 4.3.1

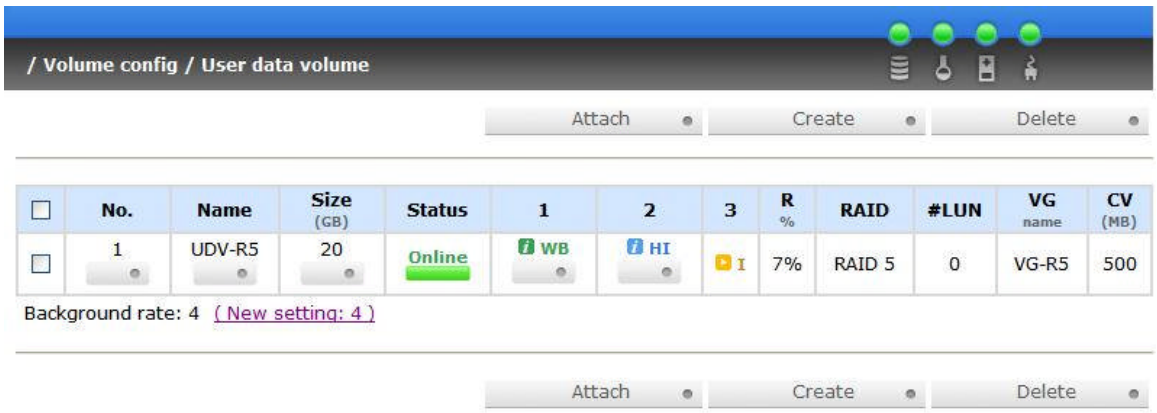


Figure 4.3.2

(Figure 4.3.2: Extend UDV-R0 from 5GB to 10GB.)

Tips
The size of UDV extension must be larger than original.

Caution
UDV Extension cannot be executed during rebuild or migration.

4.4 Disk roaming

Physical disks can be re-sequenced in the same system or move whole physical disks from system-1 to system-2. This is called disk roaming. Disk roaming has some constraints as described in the following:

1. Check the firmware of two systems first. It is better that both have same firmware version or newer.
2. Whole physical disks of related VG should be moved from system-1 to system-2 together. The configuration of both VG and UDV will be kept but LUN configuration will be cleared to avoid conflict with system-2.

4.5 Support Microsoft MPIO and MC/S

MPIO (Multi-Path Input/Output) and MC/S (Multiple Connections per Session) both use multiple physical paths to create logical "paths" between the server and the ISC8P2G. In the case where one or more of these components fail, causing the path to fail, multi-path logic uses an alternate path for I/O so that applications can still access their data.

Microsoft iSCSI initiator supports multi-path function. Please follow the procedures to use MPIO feature.

1. A host with dual LAN ports will connect to the LAN ports on the ISC8P2G.
2. Create a VG/UDV, attach this UDV to the host.
3. When installing **“Microsoft iSCSI initiator”**, please install MPIO driver at the same time.
4. Logon to the target separately for each port. When logging on to target, check “Enable multi-path”. Please refer to Appendix D, step 6.
5. MPIO mode can be selected on Targets à Details à Devices à Advanced.
6. Rescan disk.
7. There will be one disk running MPIO.

For detailed setup steps, please refer to Appendix F: MPIO and MC/S setup instructions. MC/S setup steps are very similar to MPIO, please also refer to Appendix: F.

Appendix

A. Certification list

- **RAM**

  ISC8P2G RAM Spec: 184pins, DDR333(PC2700), Reg.(register) or UB(Unbufferred), ECC or Non-ECC, from 64MB to 1GB, 32-bit or 64-bit data bus width, x8 or x16 devices, 9 to 11 bits column address.

- **iSCSI Initiator (Software)**

OS	Software/Release Number
Microsoft Windows	Microsoft iSCSI Software Initiator Release v2.05 System Requirements: 1. Windows XP Professional with SP2 2. Windows 2000 Server with SP4 3. Windows Server 2003 with SP1 4. Windows Server 2003 R2
Linux	The iSCSI Initiators are different for different Linux Kernels. 1. For Red Hat Enterprise Linux 3 (Kernel 2.4), install linux-iscsi-3.6.3.tar 2. For Red Hat Enterprise Linux 4 (Kernel 2.6), use the build-in iSCSI initiator iscsi-initiator-utils-4.0.3.0-4 in kernel 2.6.9 3. For Red Hat Enterprise Linux 5 (Kernel 2.6), use the build-in iSCSI initiator iscsi-initiator-utils-6.2.0.695-0.7.e15 in kernel 2.6.18
Mac	ATTO XTEND 2.0x SAN / Mac iSCSI Initiator GlobalSAN iSCSI Initiator v3.0 System Requirements: 1. Mac® OS X v10.3.5 or later

For ATTO initiator, it is not free. Please contact your local distributor for ATTO initiator.

- **iSCSI HBA card**

Vendor	Model
Adaptec	ASC-7211C (PCI-X, Gigabit, 1 port, TCP/IP offload, iSCSI offload)
HP	NC380T (PCI-Express, Gigabit, 2 ports, TCP/IP offload, iSCSI offload)
QLogic	QLA4010C (PCI-X, Gigabit, 1 port, TCP/IP offload, iSCSI offload)
QLogic	QLA4052C (PCI-X, Gigabit, 2 ports, TCP/IP offload, iSCSI offload)

For detailed setup steps of Qlogic QLA4010C, please refer to Appendix G: QLogic QLA4010C setup instructions.

- **NIC**

Vendor	Model
D-Link	DGE-530T (PCI, Gigabit, 1 port)
HP	NC7170 (PCI-X, Gigabit, 2 ports)
HP	NC360T (PCI-Express, Gigabit, 2 ports, TCP/IP offload)
IBM	NetXtreme 1000 T (73P4201) (PCI-X, Gigabit, 2 ports, TCP/IP offload)
Intel	PWLA8490MT (PCI-X, Gigabit, 1 port, TCP/IP offload)
Intel	PWLA8492MT (PCI-X, Gigabit, 2 ports, TCP/IP offload)
Intel	PWLA8494MT (PCI-X, Gigabit, 4 ports, TCP/IP offload)

- **GbE Switch**

Vendor	Model
Dell	PowerConnect 5324
Dell	PowerConnect 2724
Dell	PowerConnect 2708
HP	ProCurve 1800-24G
D-Link	DGS-3024

- **Hard drive**

ISC8P2G support SATA I, II disks.

Vendor	Model
Hitachi	Deskstar 7K250, HDS722580VLSA80, 80GB, 7200RPM, SATA, 8M
Hitachi	Deskstar 7K80, HDS728080PLA380, 80GB, 7200RPM, SATA II, 8M

Hitachi	Deskstar E7K500, HDS725050KLA360, 500G, 7200RPM, SATA II, 16M
Hitachi	Deskstar 7K80, HDS728040PLA320, 40G, 7200RPM, SATA II, 2M
Hitachi	Deskstar T7K500, HDT725032VLA360, 320G, 7200RPM, SATA II, 16M
Maxtor	DiamondMax Plus 9, 6Y080M0, 80G, 7200RPM, SATA, 8M
Maxtor	DiamondMax 11, 6H500F0, 500G, 7200RPM, SATA 3.0Gb/s, 16M
Samsung	SpinPoint P80, HDSASP0812C, 80GB •7200RPM, SATA, 8M
Seagate	Barracuda 7200.7, ST380013AS, 80G, 7200RPM, SATA 1.5Gb/s, 8M
Seagate	Barracuda 7200.7, ST380817AS, 80G, 7200RPM, SATA 1.5Gb/s, 8M, NCQ
Seagate	Barracuda 7200.8, ST3400832AS, 400G, 7200RPM, SATA 1.5Gb/s, 8M, NCQ
Seagate	Barracuda 7200.9, ST3500641AS, 500G, 7200RPM, SATA 3.0Gb/s, 16M, NCQ
Seagate	NL35, ST3400633NS, 400G, 7200RPM, SATA 3.0Gb/s, 16M
Seagate	NL35, ST3500641NS, 500G, 7200RPM, SATA 3.0Gb/s, 16M
Seagate	Barracuda ES, ST3500630NS, 500G, 7200RPM, SATA 3.0Gb/s, 16M
Seagate	Barracuda ES, ST3750640NS, 750G, 7200RPM, SATA 3.0Gb/s, 16M
Seagate	Barracuda ES.2, ST31000340NS, 1000G, 7200RPM, SATA 3.0Gb/s, 32M
Westem Digital	Caviar SE, WD800JD, 80GB, 7200RPM, SATA 3.0Gb/s, 8M
Westem Digital	Caviar SE, WD1600JD, 160GB, 7200RPM, SATA 1.5G/s , 8M
Westem Digital	Raptor, WD360GD, 36.7GB, 10000RPM, SATA 1.5Gb/s, 8M
Westem Digital	Caviar RE2, WD4000YR, 400GB, 7200RPM, SATA 1.5Gb/s, 16M, NCQ
Westem Digital	RE2, WD4000YS, 400GB, 7200RPM, SATA 3.0Gb/s, 16M
Westem Digital	Caviar RE16, WD5000AAKS, 500GB, 7200RPM, SATA 3.0Gb/s, 16M
Westem Digital	RE2, WD5000ABYS, 500GB, 7200RPM, SATA 3.0Gb/s, 16M, NCQ

B. Event notifications

- **PD/S.M.A.R.T. events**

Level	Type	Description
Info	Disk inserted	Info: Disk <slot> is inserted.
Info	Disk removed	Info: Disk <slot> is removed.
Warning	S.M.A.R.T. threshold exceed condition	Warning: Disk <slot> S.M.A.R.T. threshold exceed condition occurred for attribute of 1. read error rate 2. spin up time 3. reallocated sector count 4. seek error rate 5. spin up retries 6. calibration retries
Warning	S.M.A.R.T. information	Warning: Disk <slot>: Failure to get S.M.A.R.T information

- **Physical HW events**

Level	Type	Description
Warning	ECC error	Warning: Single-bit ECC error is detected.
Error	ECC error	Error: Multi-bit ECC error is detected.
Info	ECC DIMM Installed	Info: ECC Memory is installed.
Info	Non-ECC installed	Info: Non-ECC Memory is installed.
Error	Host chip failure	Error: Host channel chip failed.
Error	Drive chip failure	Error: Drive channel chip failed.
Warning	Ethernet port failure	Warning: GUI Ethernet port failed.

- **HDD IO events**

Level	Type	Description
Warning	Disk error	Error: Disk <slot> read block error.
Warning	Disk error	Error: Disk <slot> writes block error.
Warning	HDD failure	Error: Disk <slot> is failed.
Warning	Channel error	Error: Disk <slot> IO incomplete.

- **SES events**

Level	Type	Description
Info	SES load conf. OK	Info: SES configuration has been loaded.
Warning	SES Load Conf. Failure	Error: Failed to load SES configuration. The SES device is disabled.
Info	SES is disabled	Info: The SES device is disabled.
Info	SES is enabled	Info: The SES device is enabled

- **Environmental events**

Level	Type	Description
Info	Admin Login OK	Info: Admin login from <IP or serial console> via <Web UI or Console UI>.
Info	Admin Logout OK	Info: Admin logout from <IP or serial console> via <Web UI or Console UI>.
Info	iSCSI data port login	Info: iSCSI login from <IQN> (<IP:Port Number>) succeeds.

Warning	iSCSI data port login reject	Warning: iSCSI login from <IQN> (<IP:Port Number>) was rejected, reason of 1. initiator error 2. authentication failure 3. authorization failure 4. target not found 5. unsupported version 6. too many connections 7. missing parameter 8. session does not exist 9. target error 10. out of resources 11. unknown
Error	Thermal critical	Error: System Overheated!!! The system will do the auto shutdown immediately.
Warning	Thermal warning	Warning: System temperature is a little bit higher.
Error	Voltage critical	Error: System voltages failed!!! The system will do the auto shutdown immediately
Warning	Voltage warning	Warning: System voltage is a little bit higher/lower.
Info	PSU restore	Info: Power <number> is restored to work.
Error	PSU Fail	Error: Power <number> is out of work.
Info	Fan restore	Info: Fan <number> is restore to work.
Error	Fan Fail	Error: Fan <number> is out of work.
Error	Fan non-exist	Error: System cooling fan is not installed.
Error	AC Loss	Error: AC loss for the system is detected.
Info	UPS Detection OK	Info: UPS detection succeed
Warning	UPS Detection Fail	Warning: UPS detection failed
Error	AC Loss	Error: AC loss for the system is detected
Error	UPS power low	Error: UPS Power Low!!! The system will do the auto shutdown immediately.
Info	Mgmt Lan Port Active	Info: Management LAN Port is active.
Warning	Mgmt Lan Port Failed	Warning: Fail to manage the system via the LAN Port.
Info	RTC Device OK	Info: RTC device is active.
Warning	RTC Access Failed	Warning: Fail to access RTC device
Info	Reset Password	Info: Reset Admin Password to default.
Info	Reset IP	Info: Reset network settings set to default.

- **System config events**

Level	Type	Description
Info	Sys Config. Defaults Restored	Info: Default system configurations restored.
Info	Sys NVRAM OK	Info: The system NVRAM is active.
Error	Sys NVRAM IO Failed	Error: Can't access the system NVRAM.
Warning	Sys NVRAM is full	Warning: The system NVRAM is full.

- **System maintenance events**

Level	Type	Description
Info	Firmware Upgraded	Info: System firmware has been upgraded
Error	Firmware Upgraded Failed	Error: System firmware upgrade failed.
Info	System reboot	Info: System has been rebooted
Info	System shutdown	Info: System has been shutdown.
Info	System Init OK	Info: System has been initialized OK.
Error	System Init Failed	Error: System cannot be initialized in the last boot up.

- **LVM events**

Level	Type	Description
Info	VG Created OK	Info: VG <name> has been created.
Warning	VG Created Fail	Warning: Fail to create VG <name>.
Info	VG Deleted	Info: VG <name> has been deleted.
Info	UDV Created OK	Info: UDV <name> has been created.
Warning	UDV Created Fail	Warning: Fail to create UDV <name>.
Info	UDV Deleted	Info: UDV <name> has been deleted.
Info	UDV Attached OK	Info: UDV <name> has been LUN-attached.
Warning	UDV Attached Fail	Warning: Fail to attach LUN to UDV <name>.
Info	UDV Detached OK	Info: UDV <name> has been detached.
Warning	UDV Detached Fail	Warning: Fail to detach LUN from Bus <number> SCSI_ID <number> LUN <number>.
Info	UDV_OP Rebuild Started	Info: UDV <name> starts rebuilding.
Info	UDV_OP Rebuild Finished	Info: UDV <name> completes rebuilding.
Warning	UDV_OP Rebuild Fail	Warning: Fail to complete UDV <name> rebuilding.
Info	UDV_OP Migrate Started	Info: UDV <name> starts migration.
Info	UDV_OP Migrate Finished	Info: UDV <name> completes migration.
Warning	UDV_OP Migrate Failed	Warning: Fail to complete UDV <name> migration.
Warning	VG Degraded	Warning: VG <name> is under degraded mode.
Warning	UDV Degraded	Warning: UDV <name> is under degraded mode.
Info	UDV Init OK	Info: UDV <name> completes the initialization.
Warning	UDV_OP Stop Initialization	Warning: Fail to complete UDV <name> initialization.
Warning	UDV IO Fault	Error: IO failure for stripe number <number> in UDV <name>.
Warning	VG Failed	Error: Fail to access VG <name>.
Warning	UDV Failed	Error: Fail to access UDV <name>.

Warning	Global CV Adjustment Failed	Error: Fail to adjust the size of the global cache.
Info	Global Cache	Info: The global cache is OK.
Error	Global CV Creation Failed	Error: Fail to create the global cache.
Info	UDV Rename	Info: UDV <name> has been renamed as <name>.
Info	VG Rename	Info: VG <name> has been renamed as <name>.
Info	Set VG Dedicated Spare Disks	Info: Assign Disk <slot> to be VG <name> dedicated spare disk.
Info	Set Global Disks	Info: Assign Disk <slot> to the Global Spare Disks.
Info	UDV Read-Only	Info: UDV <name> is a read-only volume.
Info	WRBK Cache Policy	Info: Use the write-back cache policy for UDV <name>.
Info	WRTHRU Cache Policy	Info: Use the write-through cache policy for UDV <name>.
Info	High priority UDV	Info: UDV <name> is set to high priority.
Info	Mid Priority UDV	Info: UDV <name> is set to mid priority.
Info	Low Priority UDV	Info: UDV <name> is set to low priority.
Error	PD configuration read/write error	Error: PD <slot> lba <#> length <#> config <read | write> failed.
Error	PD read/write error	Error: PD <#> lba <#> length <#> <read | write> error.
Error	UDV recoverable read/write error	Error: UDV <name> stripe <#> PD <#> lba <#> length <#> <read | write> recoverable
Error	UDV unrecoverable read/write error	Error: UDV <#> stripe <#> PD <#> lba <#> length <#> <read | write> unrecoverable
Info	UDV stripe rewrite start/fail/succeed	Info: UDV <name> stripe <#> rewrite column bitmap <BITMAP> <started | failed | finished>.

C. Known issues

1. Microsoft MPIO is not supported on Windows XP or Windows 2000 Professional.

   Workaround solution: Using Windows Server 2008, 2003 or Windows 2000 server to run MPIO.

D. Microsoft iSCSI Initiator

Here is the step-by-step procedure to setup Microsoft iSCSI Initiator. Please visit Microsoft website for latest iSCSI initiator.

1. Run Microsoft iSCSI Initiator version 2.07. Please see Figure D.1.
2. Click **"Discovery"**.

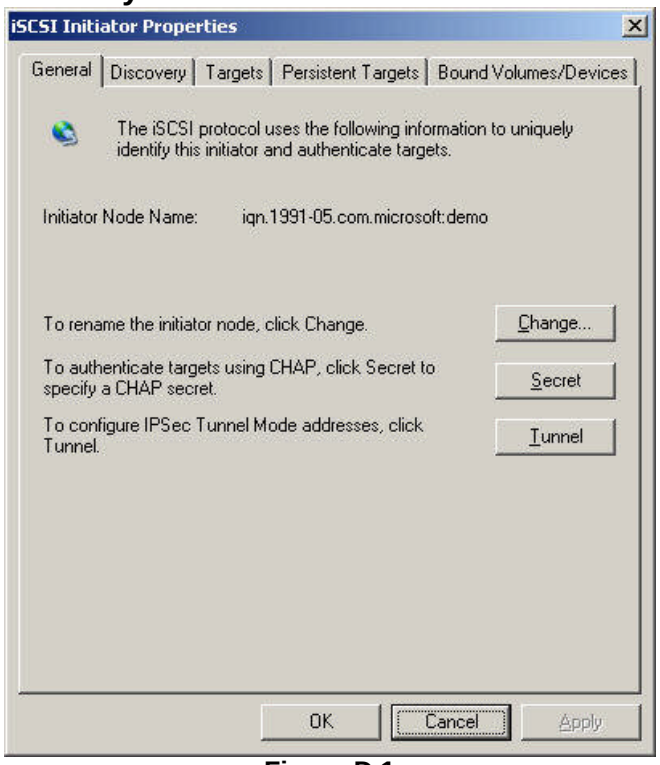


Figure D.1

3. Click **"Add"**. Input IP address or DNS name of ISC8P2G. Please see Figure D.2.

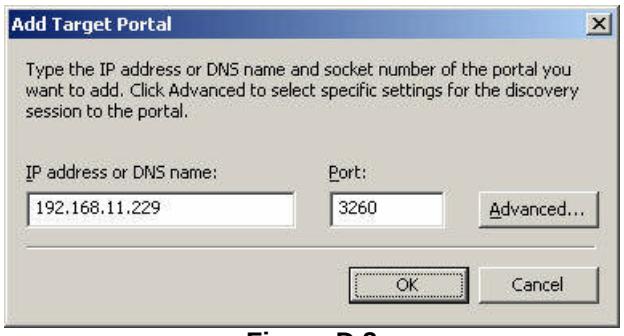

Add Target Portal
Type the IP address or DNS name and socket number of the portal you want to add. Click Advanced to select specific settings for the discovery session to the portal.
IP address or DNS name:
Port:
192.168.11.229
3260
Advanced...
OK
Cancel

Figure D.2

4. Click **“OK”**. Please see Figure D.3.

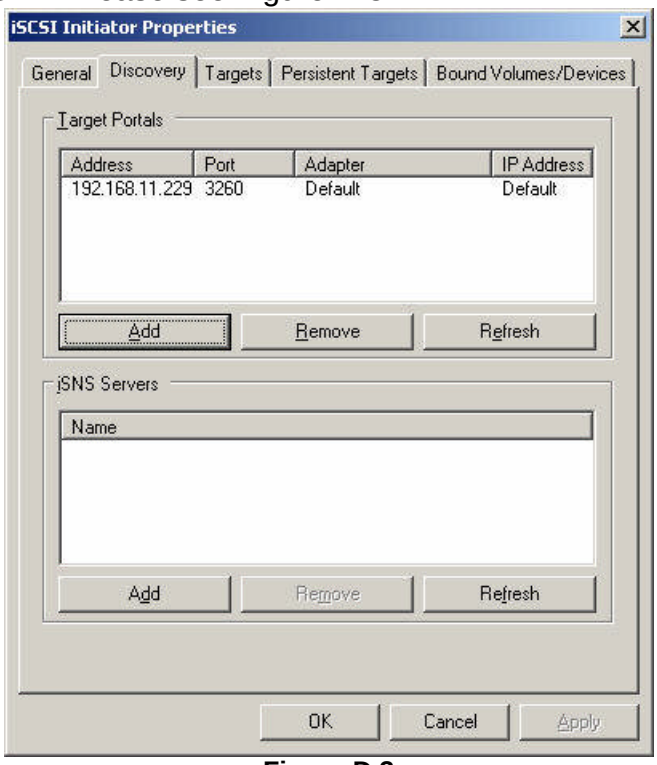


Figure D.3

5. Click **“Targets”**. Please see Figure D.4.

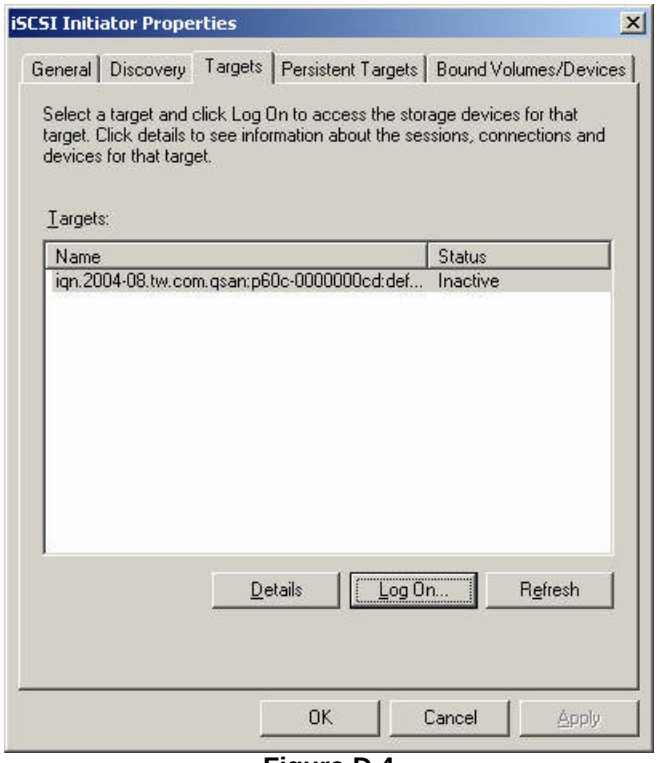


Figure D.4

6. Click **“Log On”**. Please see Figure D.5. Check **“Enable multi-path”** if running MPIO.

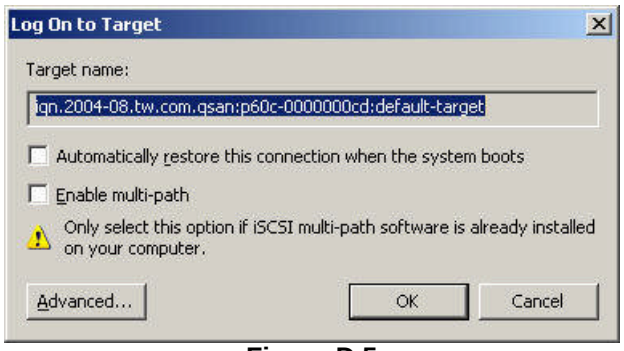


Figure D.5

7. Click **“Advance…”** if CHAP information is needed. Please see Figure D.6.

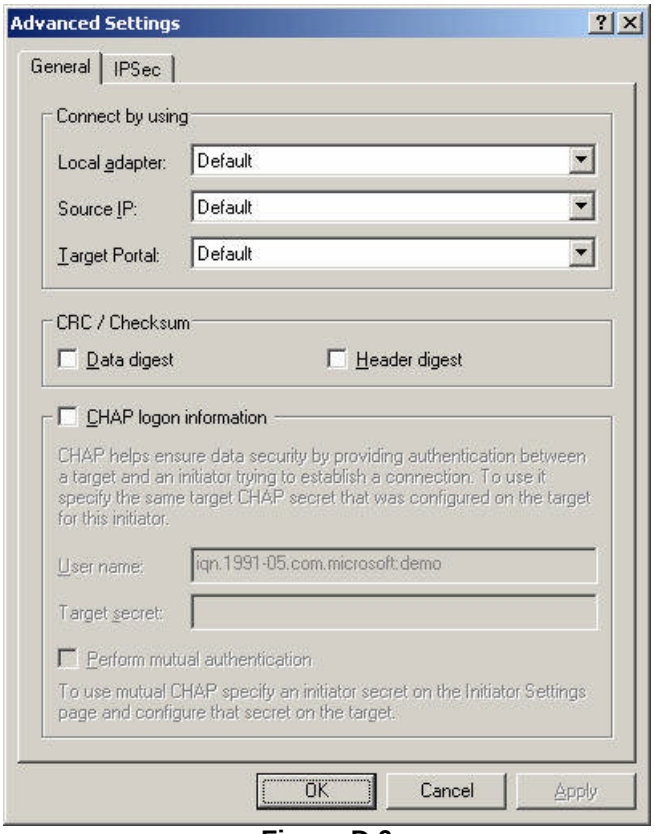

Advanced Settings
General
IPSec
Connect by using
Local adapter:
Default
Source IP:
Default
Target Portal:
Default
CRC / Checksum
Data digest
Header digest
CHAP logon information
CHAP helps ensure data security by providing authentication between a target and an initiator trying to establish a connection. To use it specify the same target CHAP secret that was configured on the target for this initiator.
User name:
iqn.1991-05.com.microsoft:demo
Target secret:
Perform mutual authentication
To use mutual CHAP specify an initiator secret on the Initiator Settings page and configure that secret on the target.
OK
Cancel
Apply

Figure D.6

8. Click **“OK”**. The status would be “Connected”. Please see Figure D.7.

9. Done. You can connect to the iSCSI disk.

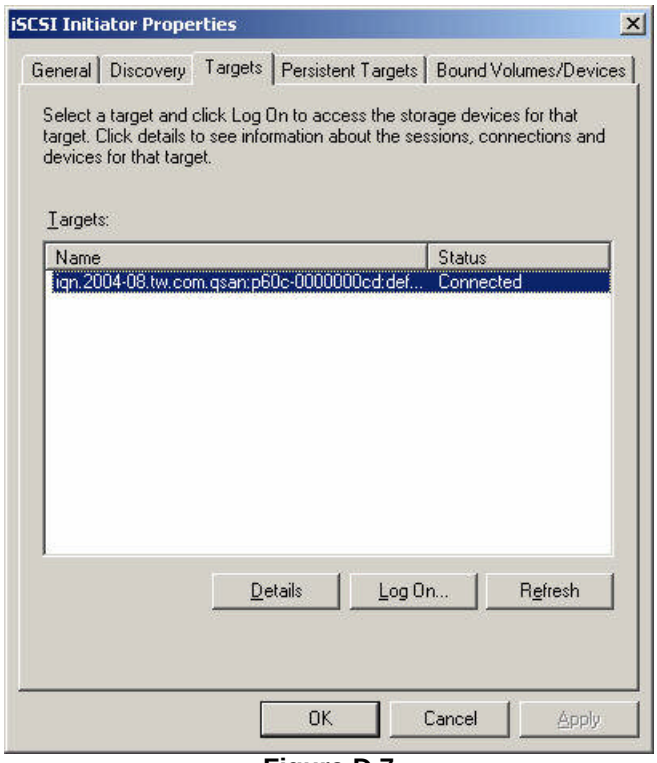


Figure D.7

The following procedure shows how to log off iSCSI drive.

1. Click **“Details”**. Please see Figure D.8.

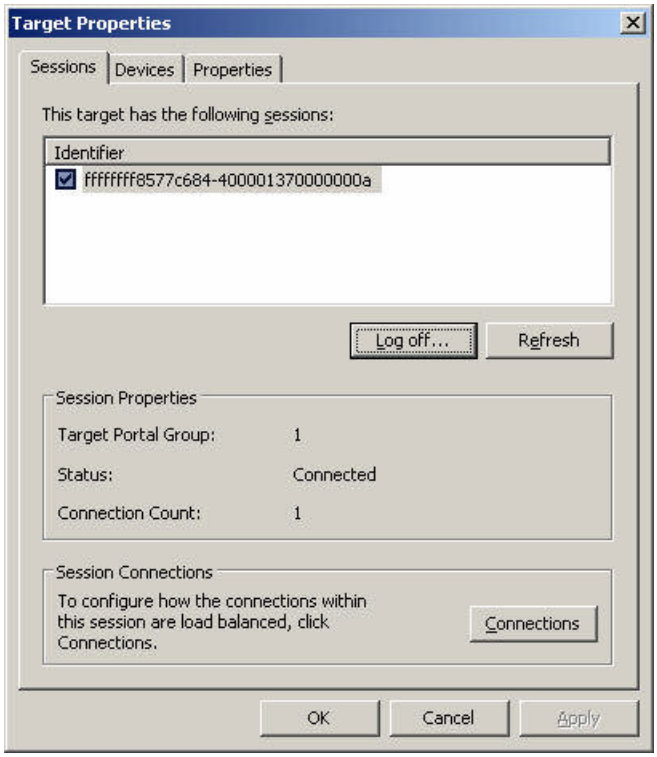


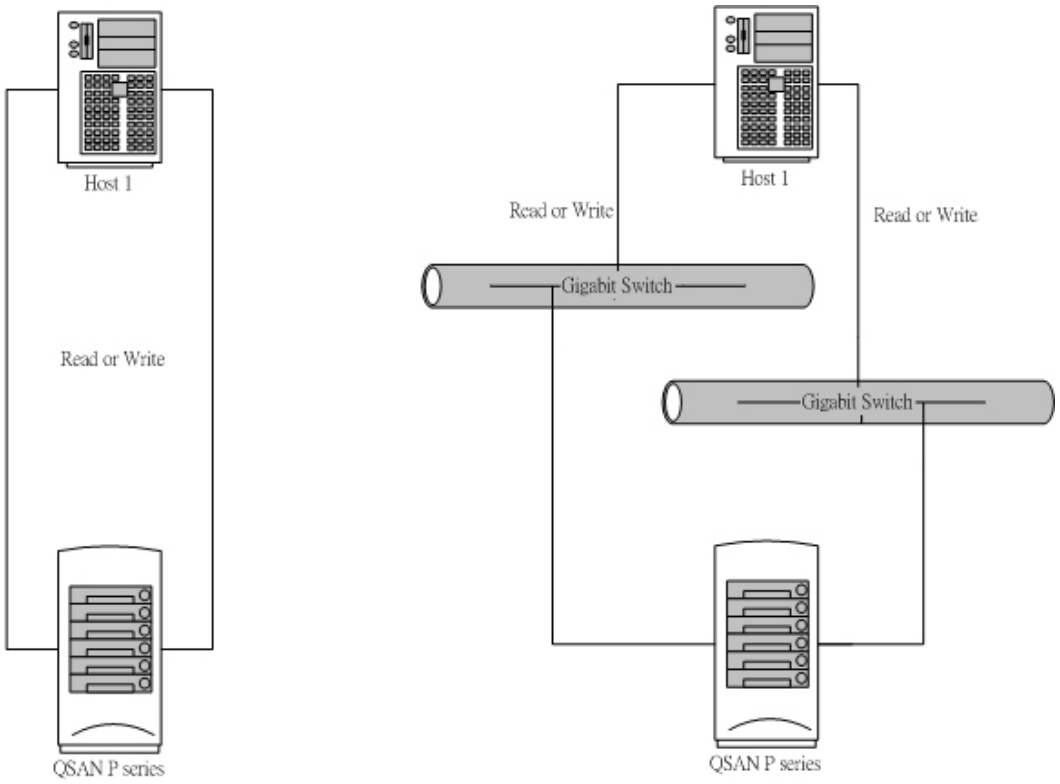
Figure D.8

2. Check the Identifier, which will be deleted.
3. Click **“Log off”**.
4. Done. The iSCSI drive was log off successfully.

E. MPIO and MC/S setup instructions

Here is the step-by-step procedure to setup MPIO. There are 2 kinds of scenarios for MPIO. Please see Figure F.1. We suggest using scenario 2 for better performance.

- Network diagram of MPIO.



1. Dual ports with MPIO (Direct connect, host has 2 LAN ports, read or write in one UDV)

2. Dual ports with MPIO (Via switches, host has 2 LAN ports, read or write in one UDV)

Figure F.1

Below are the setup instructions.

Microsoft MPIO is NOT supported on Windows XP or Windows 2000 Professional.

Workaround solution: Using Windows Server 2003, 2008 or Windows 2000 server to run MPIO. You have to enable MPIO or install MPIO driver on the server before doing this instruction.

On a Windows Server 2008, to install MPIO

1. In the Server Manager console tree, click Features node.
2. In the Features pane, under Features Summary, click Add Features.
3. In the Add Features wizard, select Multipath I/O check box, and click Next.
4. Follow the steps on the Add Features wizard.

1. Create a VG with RAID 5, using 3 HDDs.

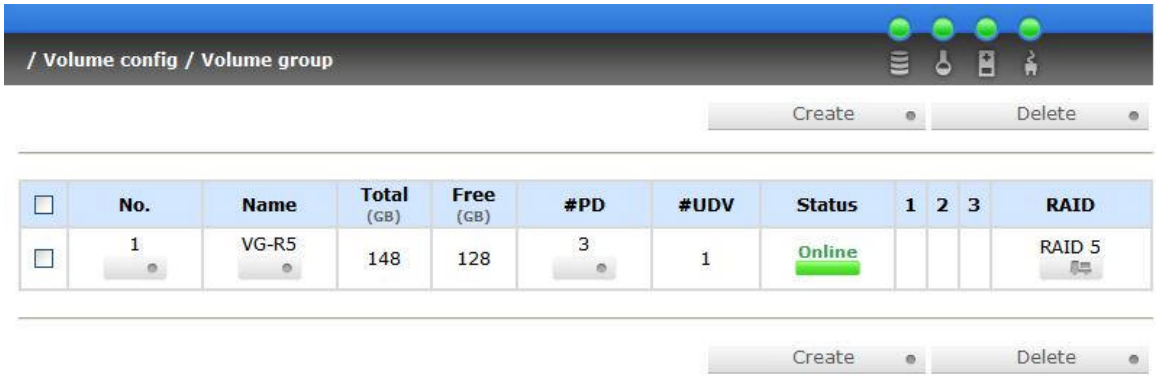


Figure F.2

2. Create a UDV by using RAID 5 VG.

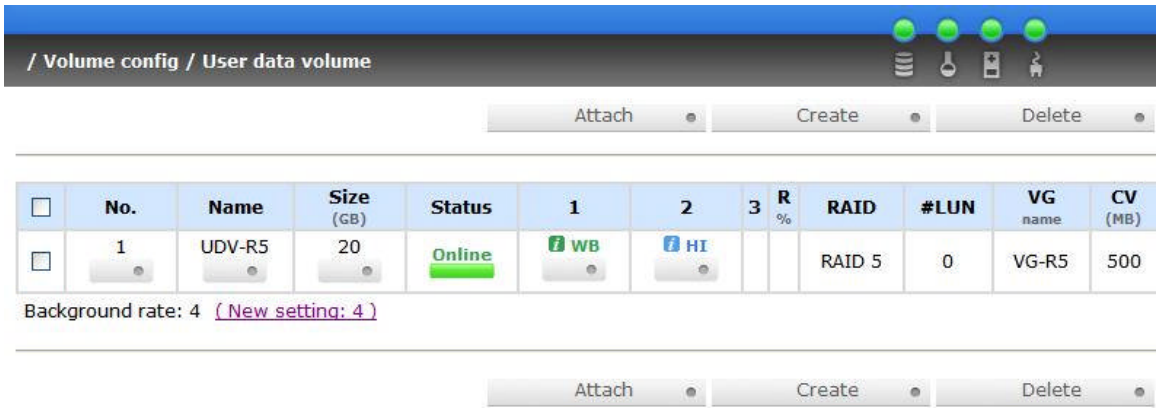


Figure F.3

3. Run Microsoft iSCSI initiator and check the Initiator Node Name.

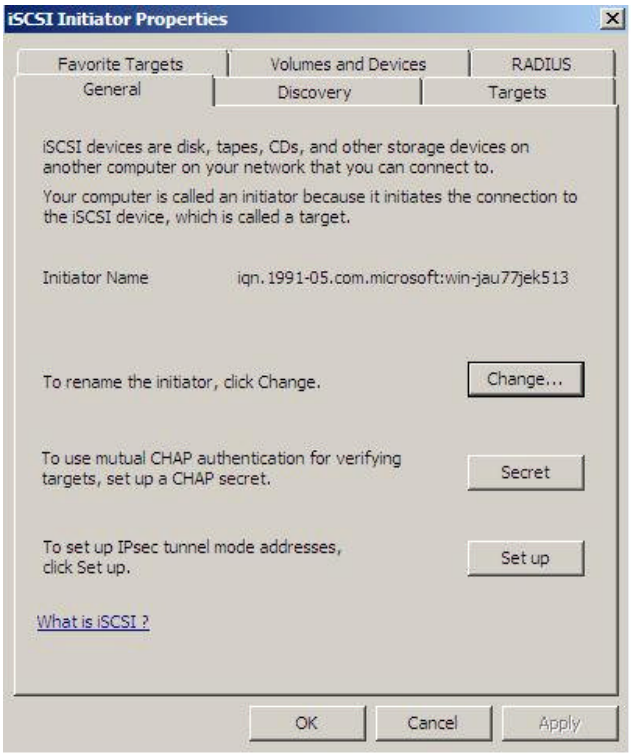

iSCSI Initiator Properties
Favorite Targets
Volumes and Devices
RADIUS
General
Discovery
Targets
iSCSI devices are disk, tapes, CDs, and other storage devices on another computer on your network that you can connect to.
Your computer is called an initiator because it initiates the connection to the iSCSI device, which is called a target.
Initiator Name
iqn.1991-05.com.microsoft:win-jau77jek513
To rename the initiator, click Change.
Change...
To use mutual CHAP authentication for verifying targets, set up a CHAP secret.
Secret
To set up IPsec tunnel mode addresses, click Set up.
Set up
What is iSCSI ?
OK
Cancel
Apply

Figure F.4

4. Attached LUN to R5 UDV. Input the Initiator Node Name in Host field.

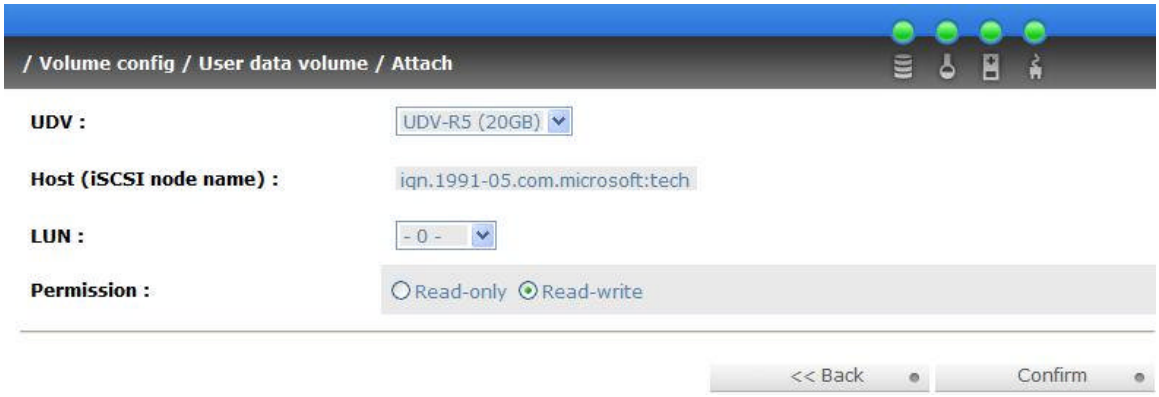


Figure F.5

5. The volume config setting is done.

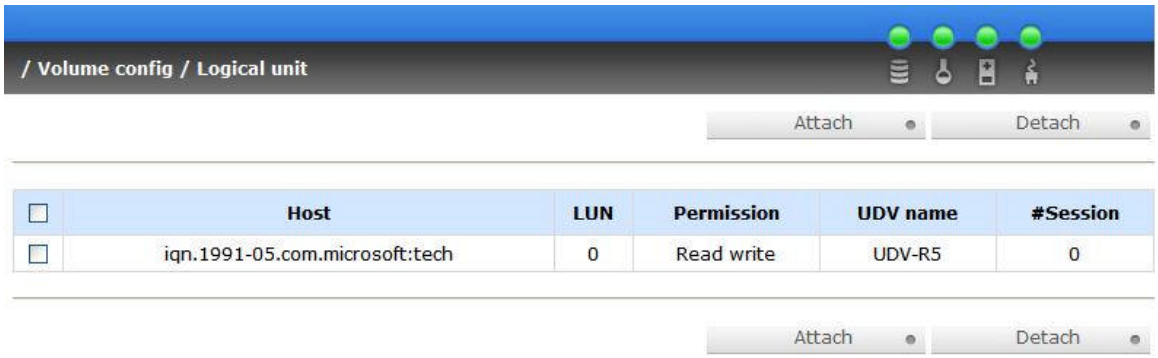


Figure F.6

6. Check iSCSI settings. The IP address of iSCSI data port 1 is 192.168.1.113, port 2 is 192.168.1.112 for example.

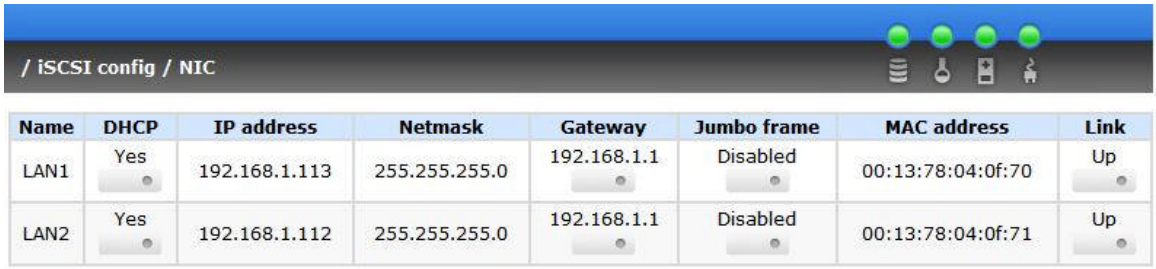


Figure F.7

7. Add Target Portals on Microsoft iSCSI initiator.

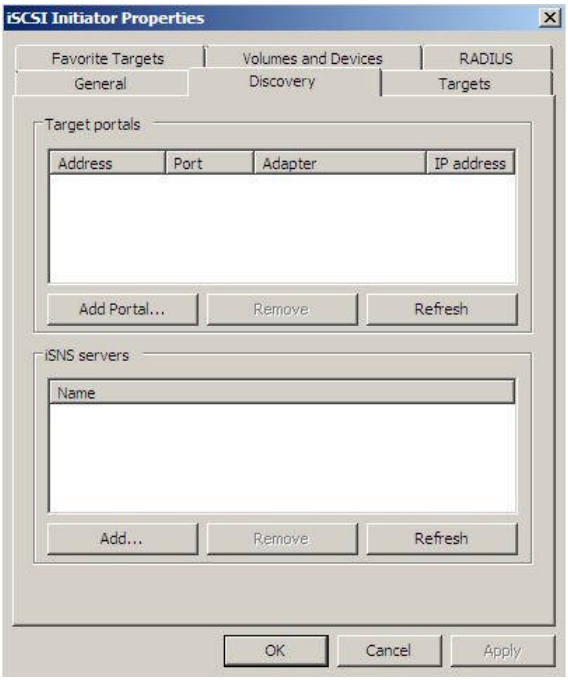


Figure F.8

8. Input the IP address of iSCSI data port 1 (192.168.1.112 as mentioned in previous page).

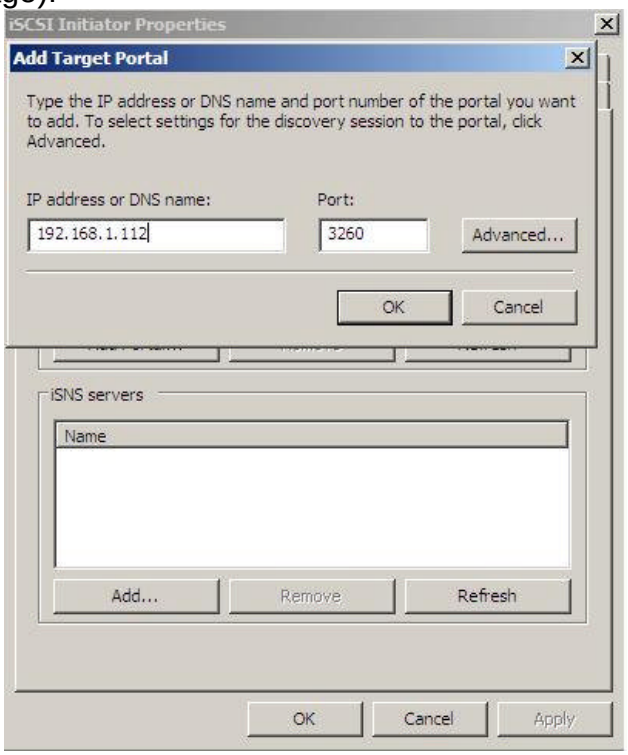


Figure F.9

9. Add second Target Portals on Microsoft iSCSI initiator.

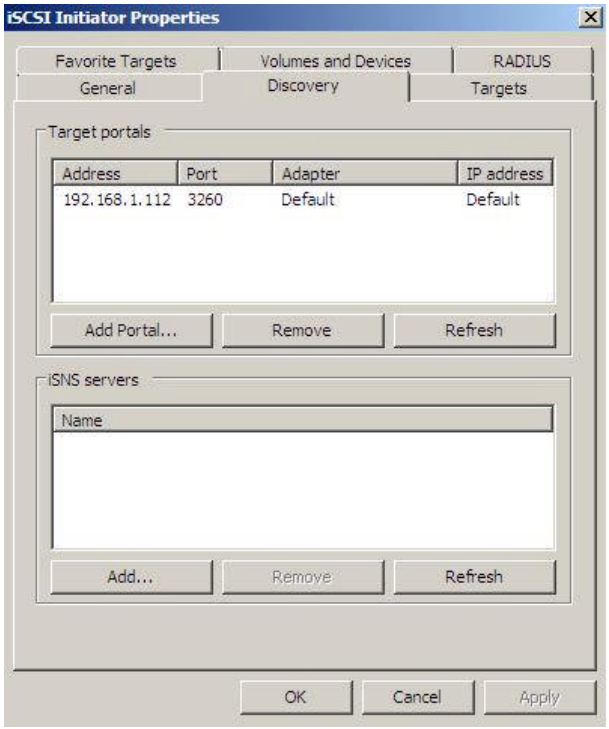


Figure F.10

10. Input the IP address of iSCSI data port 2 (192.168.1.113 as mentioned in previous page).

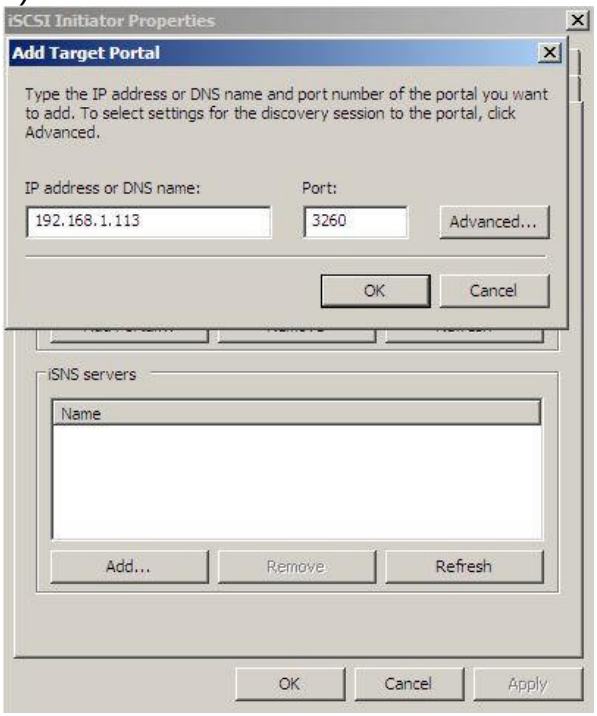


Figure F.11

11. The initiator setting is done.

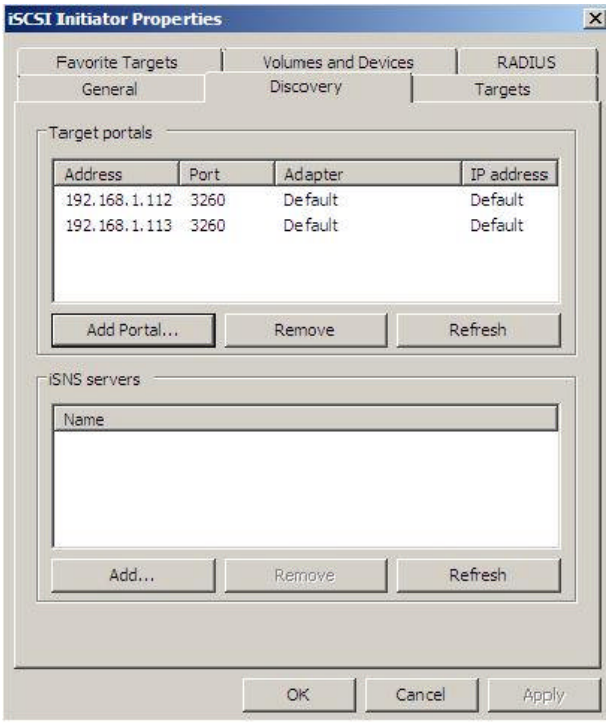


Figure F.12

12. Log on.

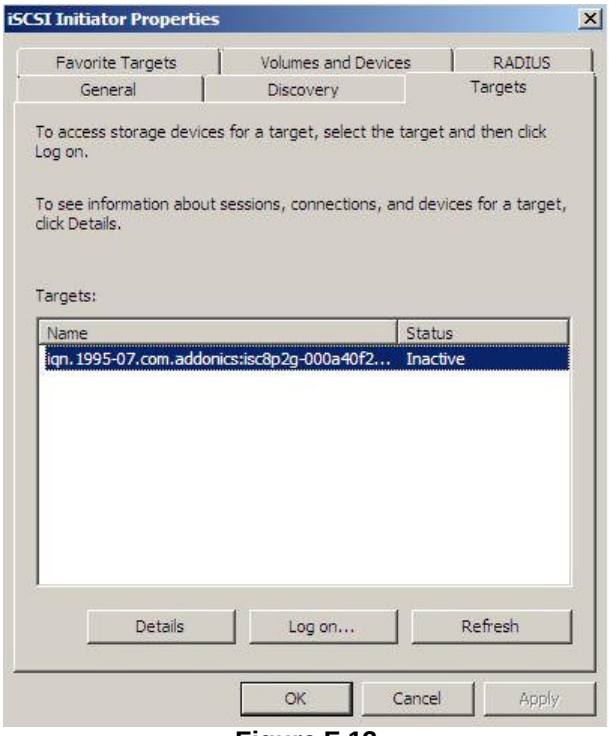


Figure F.13

13. Enable **"Enable multi-path"** checkbox. Then click **"Advanced"**.

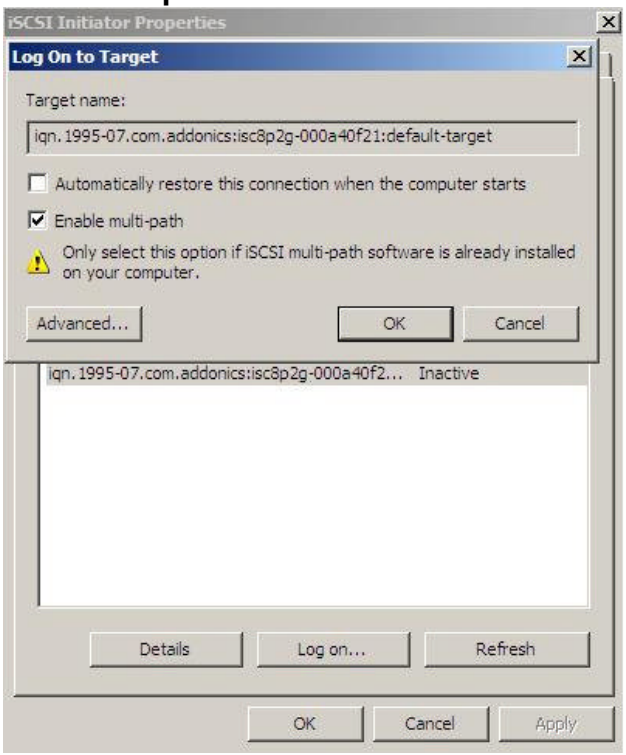


Figure F.14

14. Select Target Portal to iSCSI data port 1 (192.168.1.112). Then click **“OK”**

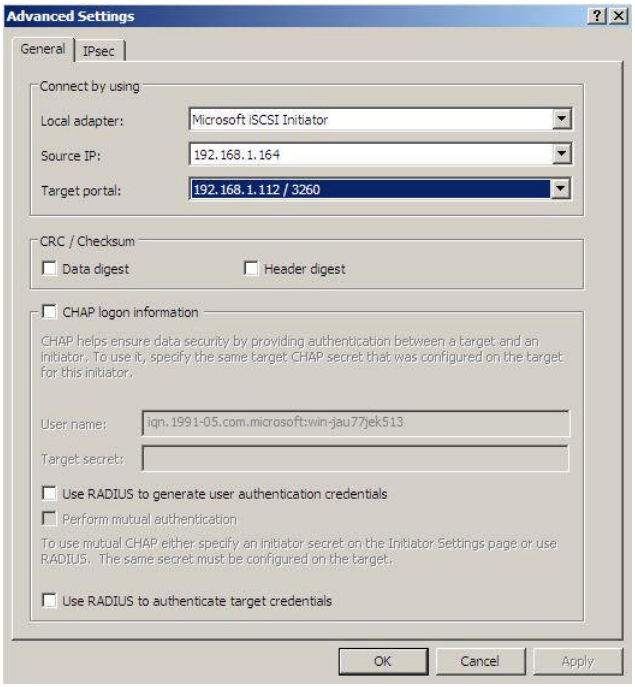

Advanced Settings
General
IPsec
Connect by using
Local adapter:
Microsoft iSCSI Initiator
Source IP:
192.168.1.164
Target portal:
192.168.1.112 / 3260
CRC / Checksum
Data digest
Header digest
CHAP logon information
CHAP helps ensure data security by providing authentication between a target and an initiator. To use it, specify the same target CHAP secret that was configured on the target for this initiator.
User name:
iqn.1991-05.com.microsoft:win-jau77jek513
Target secret:
Use RADIUS to generate user authentication credentials
Perform mutual authentication
To use mutual CHAP either specify an initiator secret on the Initiator Settings page or use RADIUS. The same secret must be configured on the target.
Use RADIUS to authenticate target credentials
OK
Cancel
Apply

Figure F.15

15. Log on **“Enable multi-path”** again.

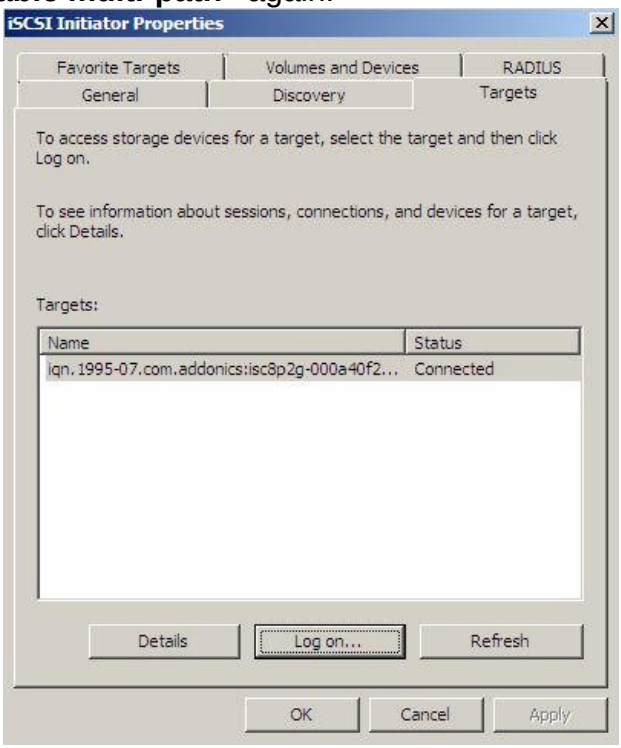


Figure F.16

16. Enable **“Enable multi-path”** checkbox. Then click **“Advanced…”**.

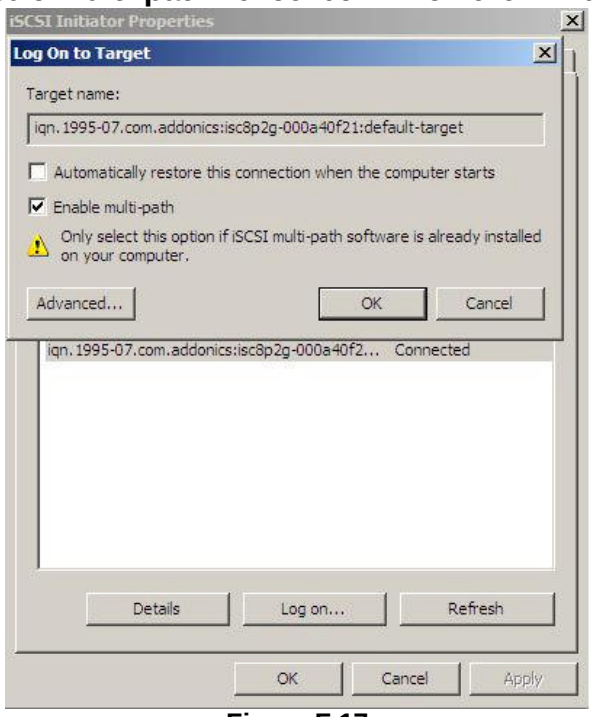


Figure F.17

17. Select Target Portal to iSCSI data port 2 (192.168.1.113). Then select **“OK”**

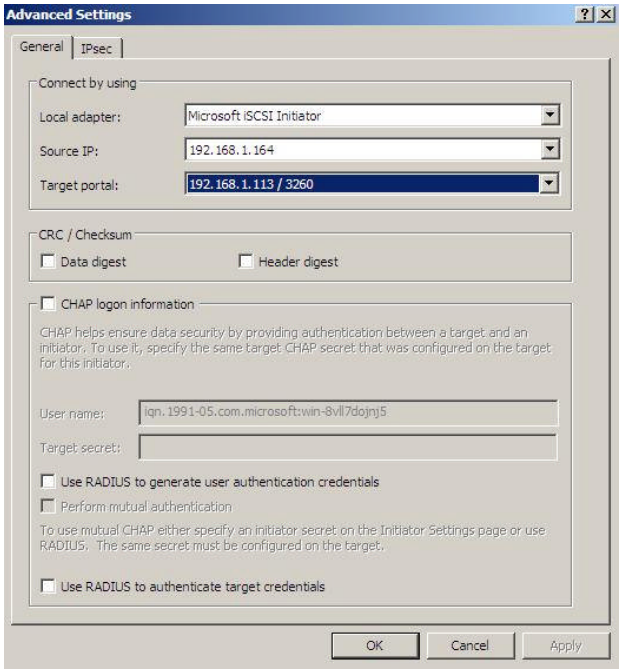
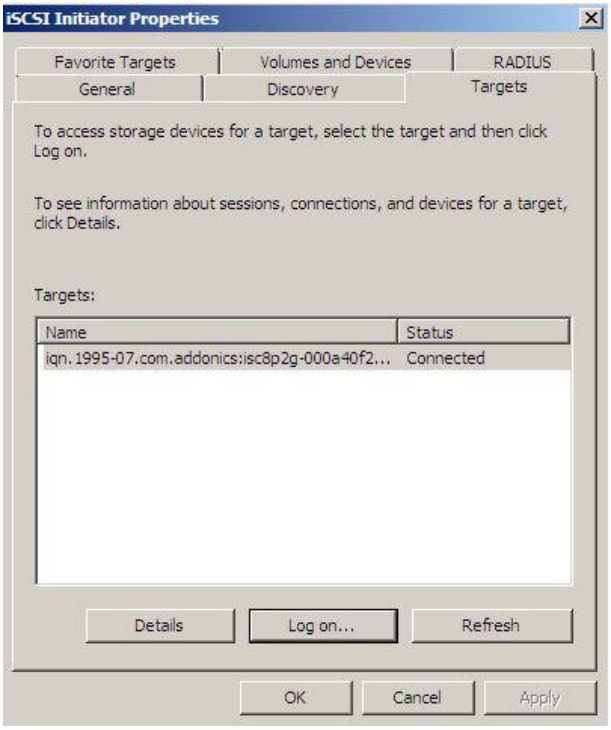
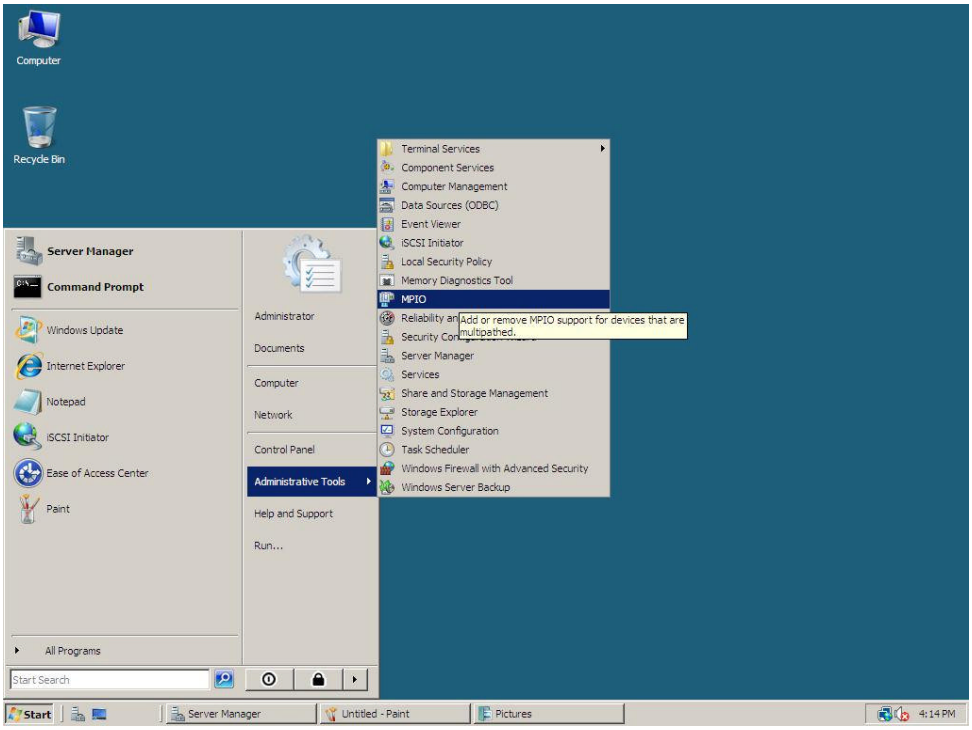

Advanced Settings
General
IPsec
Connect by using
Local adapter:
Microsoft iSCSI Initiator
Source IP:
192.168.1.164
Target portal:
192.168.1.113 / 3260
CRC / Checksum
Data digest
Header digest
CHAP logon information
CHAP helps ensure data security by providing authentication between a target and an initiator. To use it, specify the same target CHAP secret that was configured on the target for this initiator.
User name:
iqn.1991-05.com.microsoft:win-8vll7dojnj5
Target secret:
Use RADIUS to generate user authentication credentials
Perform mutual authentication
To use mutual CHAP either specify an initiator secret on the Initiator Settings page or use RADIUS. The same secret must be configured on the target.
Use RADIUS to authenticate target credentials
OK
Cancel
Apply

Figure F.18

18. The iSCSI drive is connected.



19. After the MPIO feature has been enabled, configure MPIO through the tool in Administrative Tools.



20. The MPIO Properties window opens.

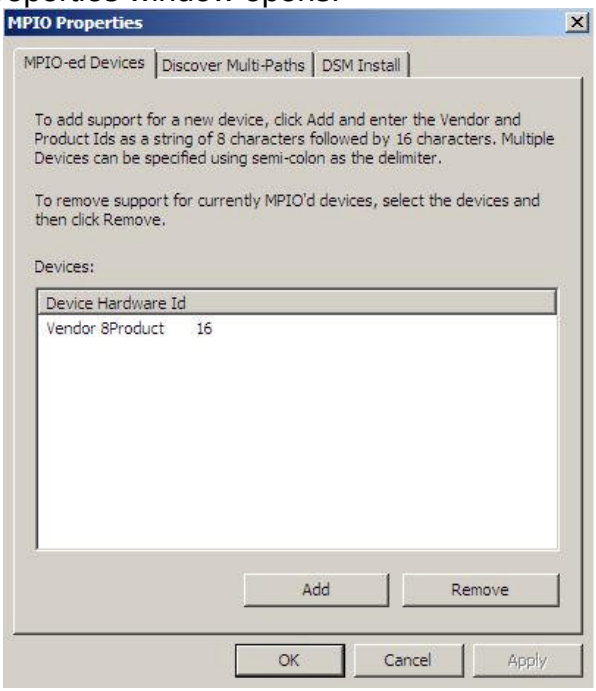

MPIO Properties
MPIO-ed Devices
Discover Multi-Paths
DSM Install
To add support for a new device, click Add and enter the Vendor and Product Ids as a string of 8 characters followed by 16 characters. Multiple Devices can be specified using semi-colon as the delimiter.
To remove support for currently MPIO'd devices, select the devices and then click Remove.
Devices:
Device Hardware Id
Vendor 8Product 16
Add
Remove
OK
Cancel
Apply

Figure F.19

21. Click on the Discover Multi-Paths tab.

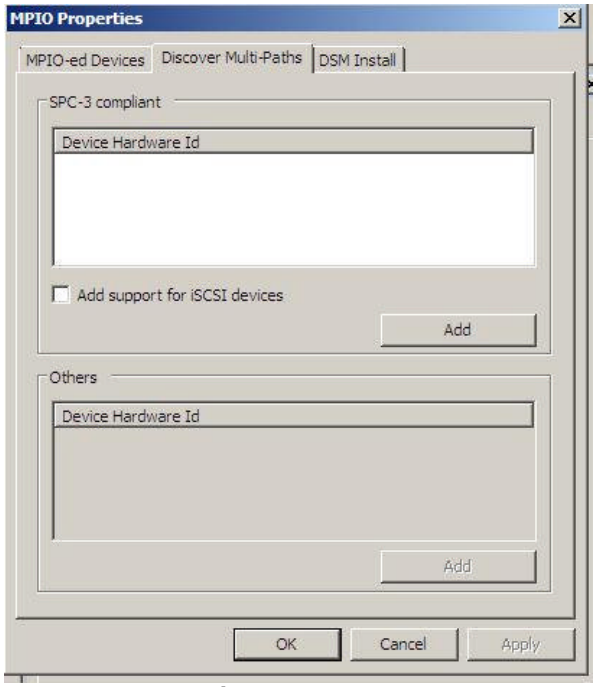


Figure F.20

22. Check the option of Add support for iSCSI device and click on Add button.

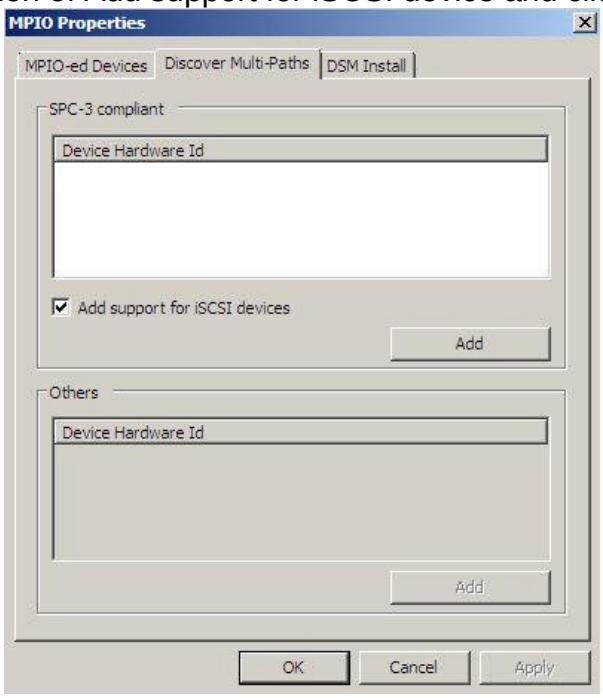


Figure F.21

23. The system will ask you to reboot to make the change take effect.

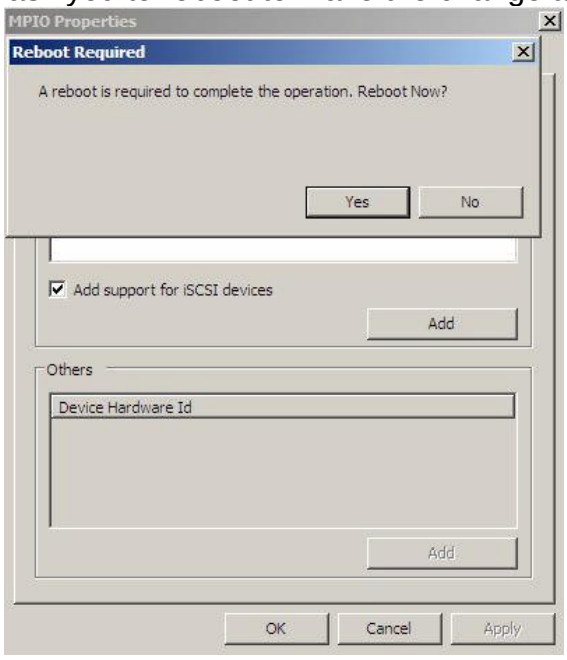


Figure F.22

24. After reboot, log on the iSCSI target again. Under Disk Driver in Device Manager, notice that the Addonics iSCSI is now a Multi-Path Disk Device.

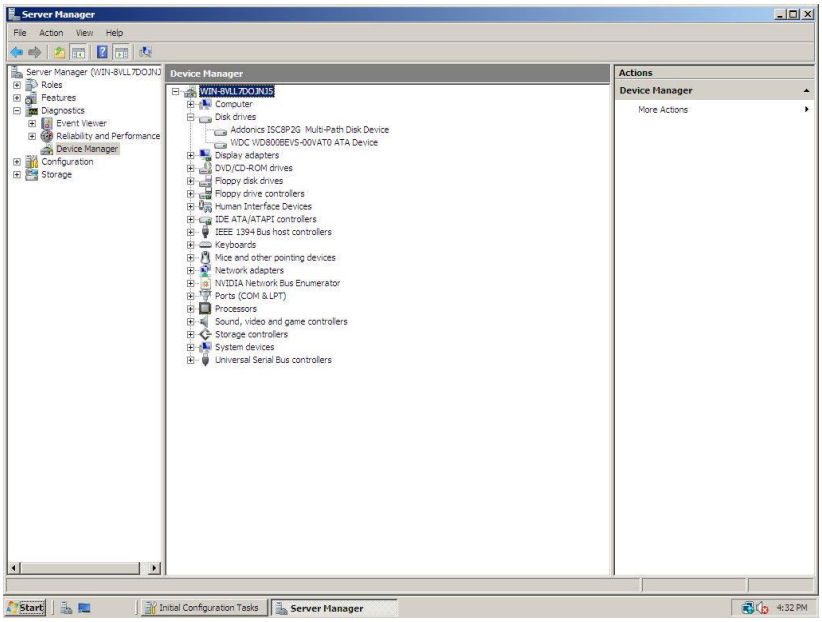


Figure F.23

25. Connect to the iSCSI device.

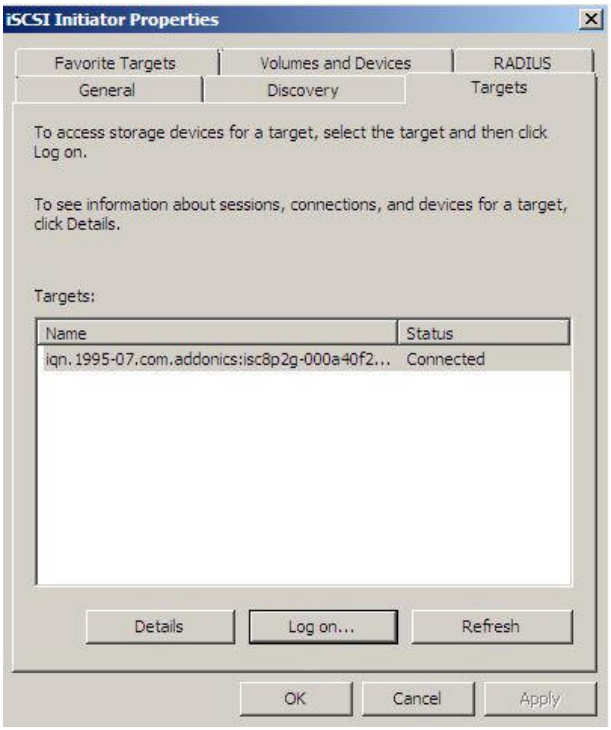


Figure F.24

26. Click **“Details”**.

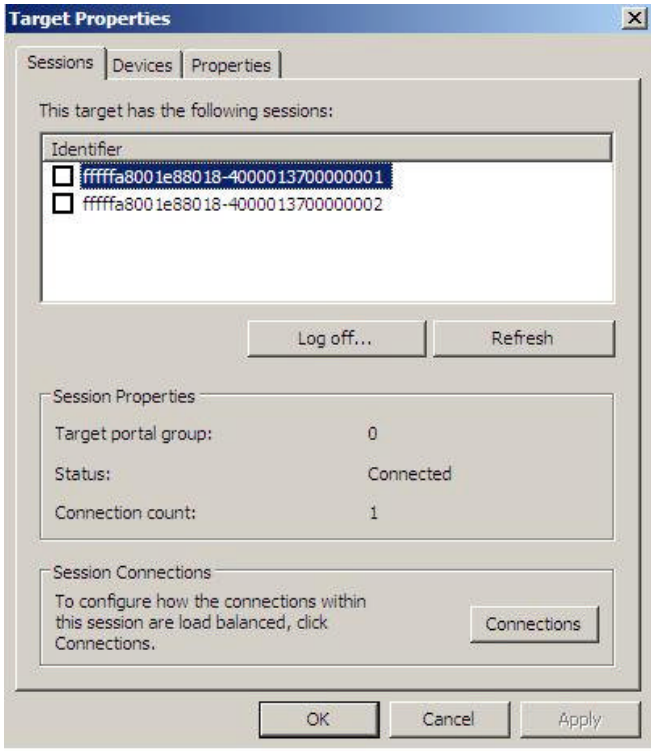


Figure F.25

27. Click **“Device”** tab, then click **“Advanced”**.

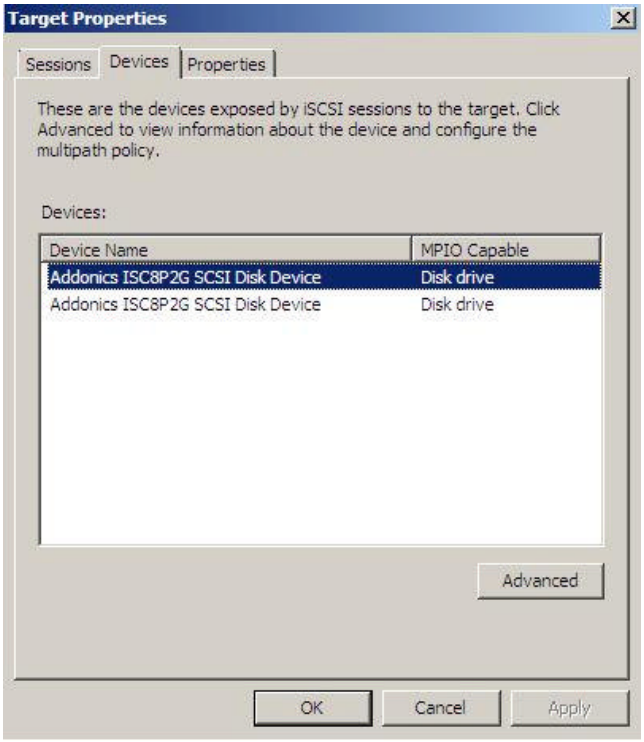


Figure F.26

28. The Device Details window opens

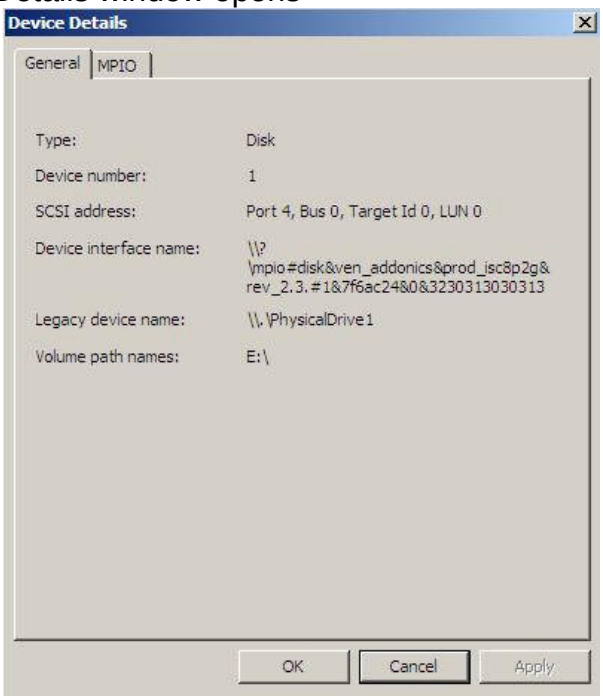


Figure F.26

29. Click **“MPIO”** tab, select **“Fail Over Only”** to **“Round Robin”**.

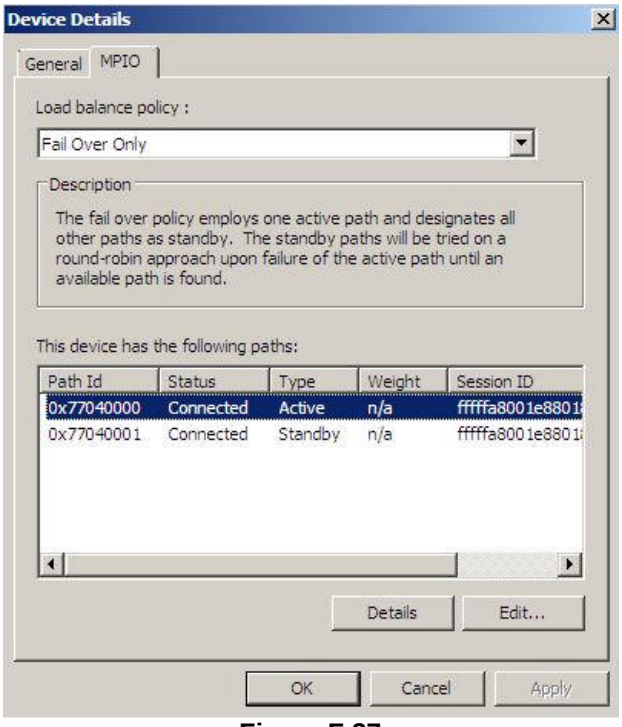


Figure F.27

30. Click **“Apply”**. Both connections Type now becomes Active.

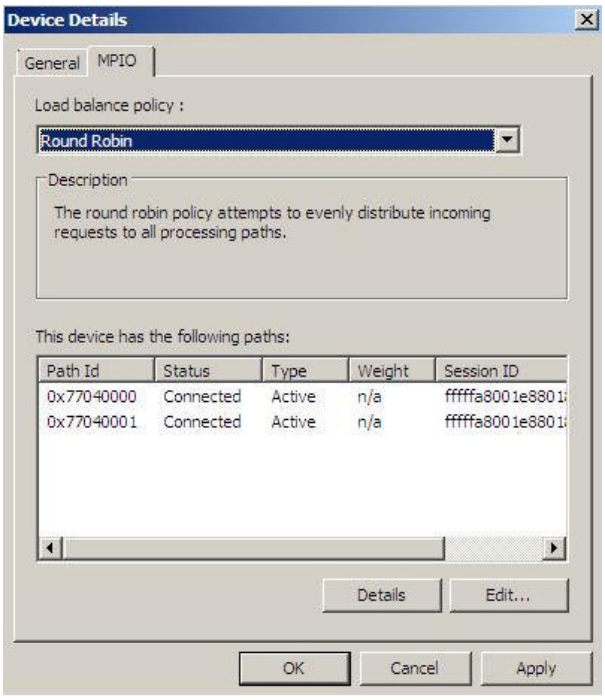


Figure F.28

The **MC/S** setup instructions are very similar to MPIO. Detailed steps are presented below. For the target side setting, the steps are exactly the same as MPIO. Please refer to **Figure F.1 to Figure F.8**.

1. Create a VG with RAID 5, using 3 HDDs.
2. Create a UDV by using RAID 5 VG.
3. Run Microsoft iSCSI initiator 2.07 and check the Initiator Node Name.
4. Attach LUN to R5 UDV. Input the Initiator Node Name in Host field.
5. The volume config setting is done.
6. Check iSCSI settings. The IP address of iSCSI data port 1 is 192.168.1.112, port 2 is 192.168.1.113 for example.
7. Add Target Portals on Microsoft iSCSI initiator 2.03.
8. Input the IP address of iSCSI data port 1 (192.168.1.112 as mentioned in previous pages). For MC/S, there is only ONE **"Target Portal"** in the **"Discovery"** tab.

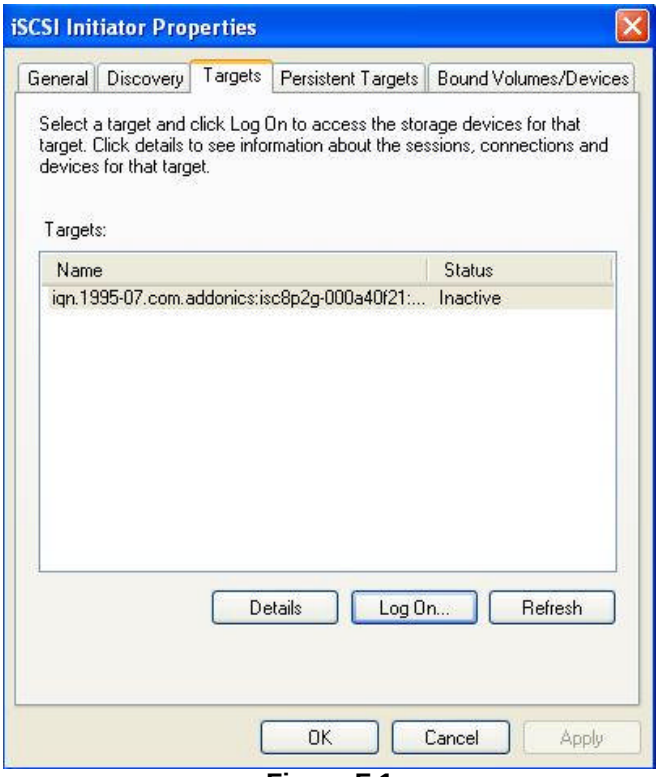


Figure F.1

9. Click Log On button.

10. Then click **“Advanced…”**.

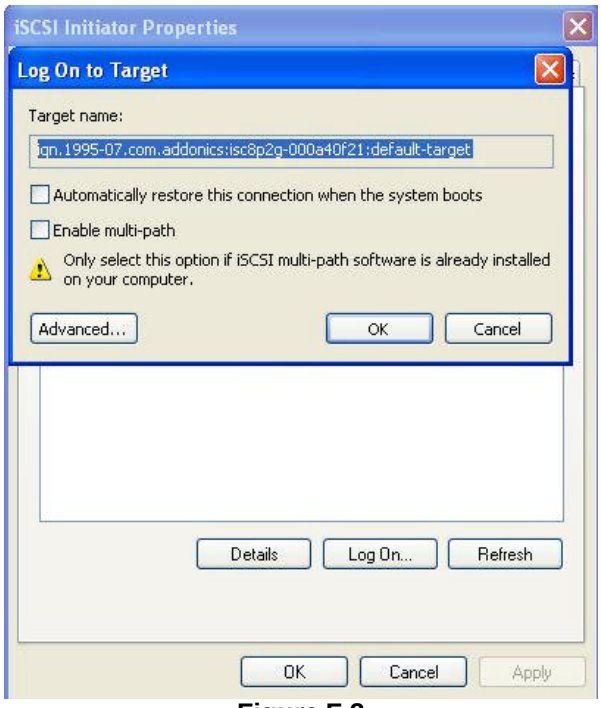


Figure F.2

11. Select Local Adapter, Source IP, and Target Portal to iSCSI data port 1 (192.168.1.112). Then click **“OK”**.

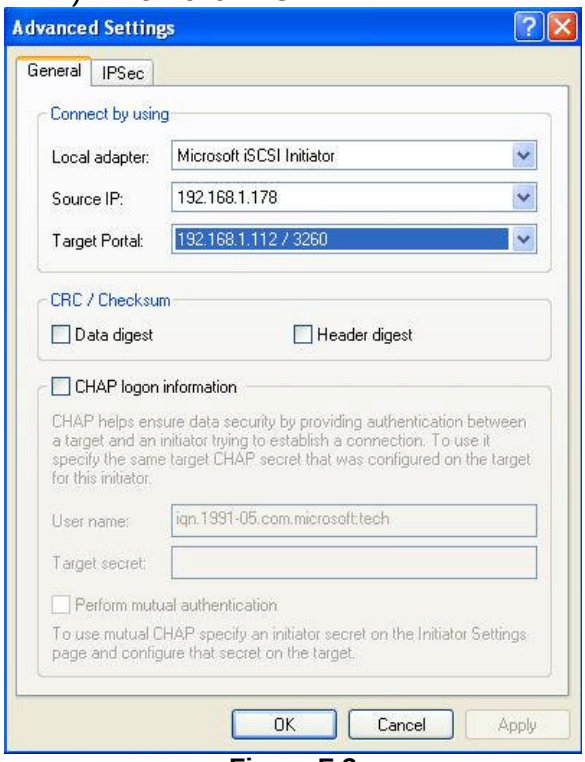

Advanced Settings
General
IPSec
Connect by using
Local adapter:
Microsoft iSCSI Initiator
Source IP:
192.168.1.178
Target Portal:
192.168.1.112 / 3260
CRC / Checksum
Data digest
Header digest
CHAP logon information
CHAP helps ensure data security by providing authentication between a target and an initiator trying to establish a connection. To use it specify the same target CHAP secret that was configured on the target for this initiator.
User name:
iqn.1991-05.com.microsoft:tech
Target secret:
Perform mutual authentication
To use mutual CHAP specify an initiator secret on the Initiator Settings page and configure that secret on the target.
OK
Cancel
Apply

Figure F.3

12. After connected, click **“Details”**, then in the **“Session”** tab, click **“Connections”**.

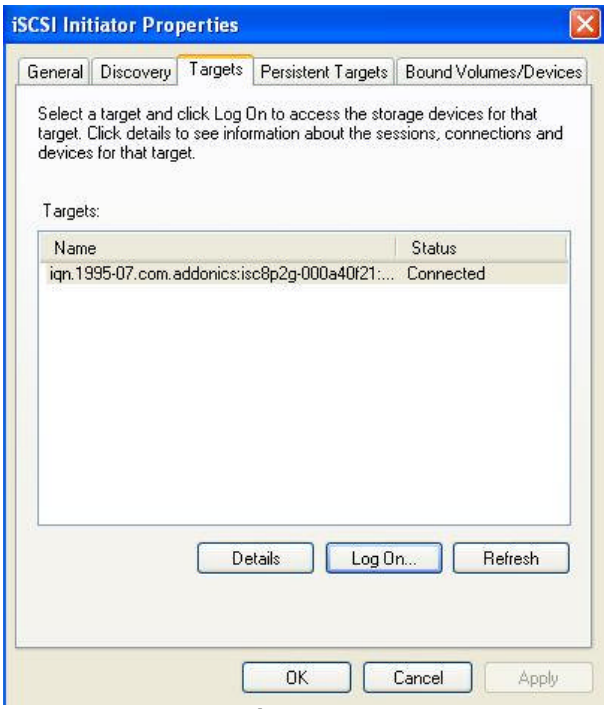


Figure F.4

13. Choose **“Round Robin”** for Load Balance Policy

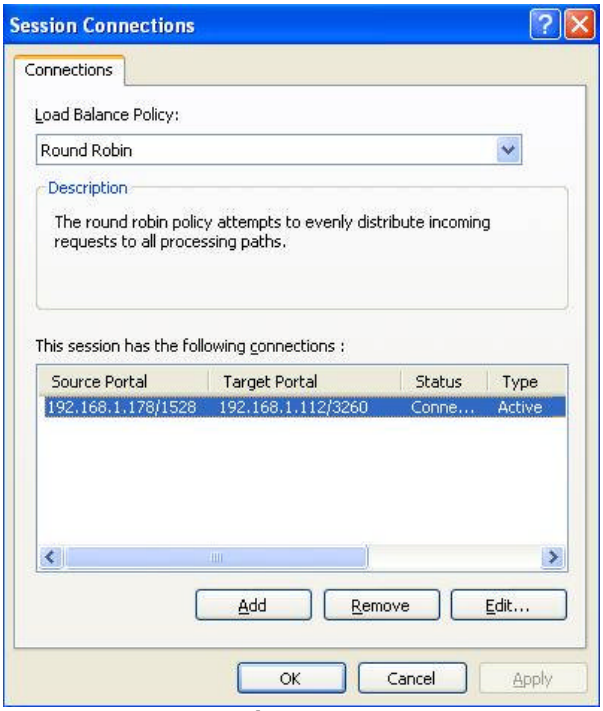


Figure F.5

14. **“Add”** Source Portal for the iSCSI data port 2(192.168.1.113)

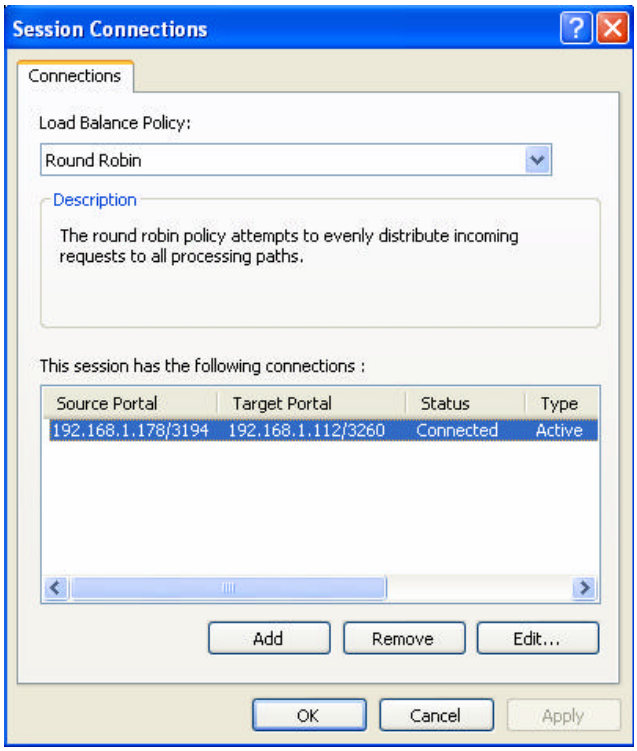


Figure F.6

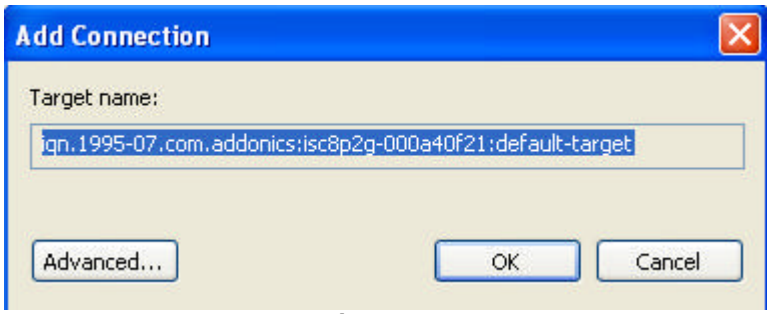


Figure F.7

15. Click on the Advance button. Select Local adapter, Source IP, and Target Portal to iSCSI data port 2 (192.168.1.113). Then select **"OK"**. Click OK.

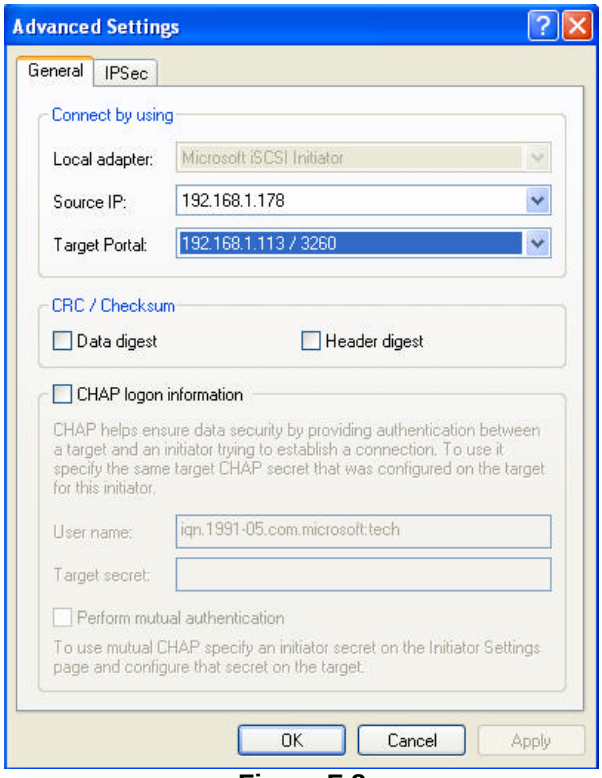
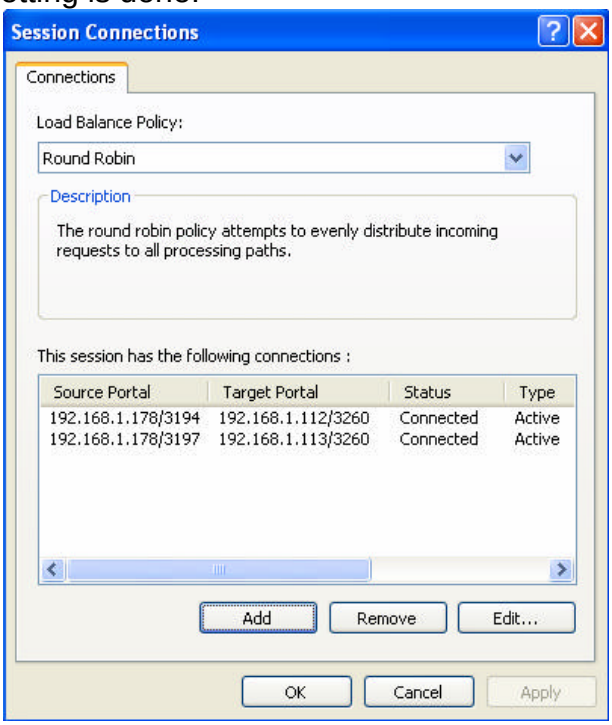

Advanced Settings
General
IPSec
Connect by using
Local adapter:
Microsoft iSCSI Initiator
Source IP:
192.168.1.178
Target Portal:
192.168.1.113 / 3260
CRC / Checksum
Data digest
Header digest
CHAP logon information
CHAP helps ensure data security by providing authentication between a target and an initiator trying to establish a connection. To use it specify the same target CHAP secret that was configured on the target for this initiator.
User name:
iqn.1991-05.com.microsoft:tech
Target secret:
Perform mutual authentication
To use mutual CHAP specify an initiator secret on the Initiator Settings page and configure that secret on the target.
OK
Cancel
Apply

Figure F.8

16. The MC/S setting is done.



E. QLogic QLA4010C setup instructions

The following is the step-by-step setup of Qlogic QLA4010C.

1. Log on the iSCSI HBA Manager and the current state shows **"No Connection Active"**.

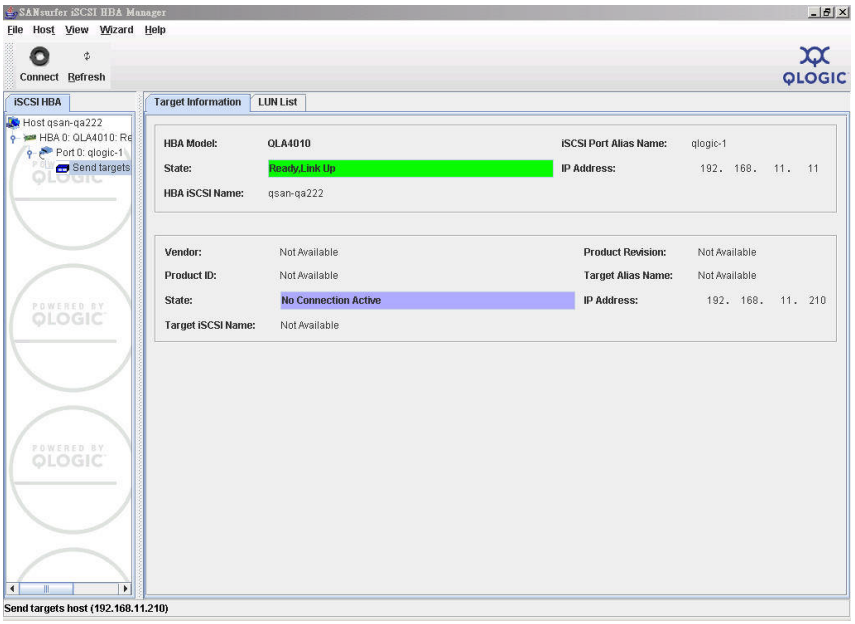


Figure G.1

2. Click **"Target settings"**. Then select the target and click **"Config Parameters"**.

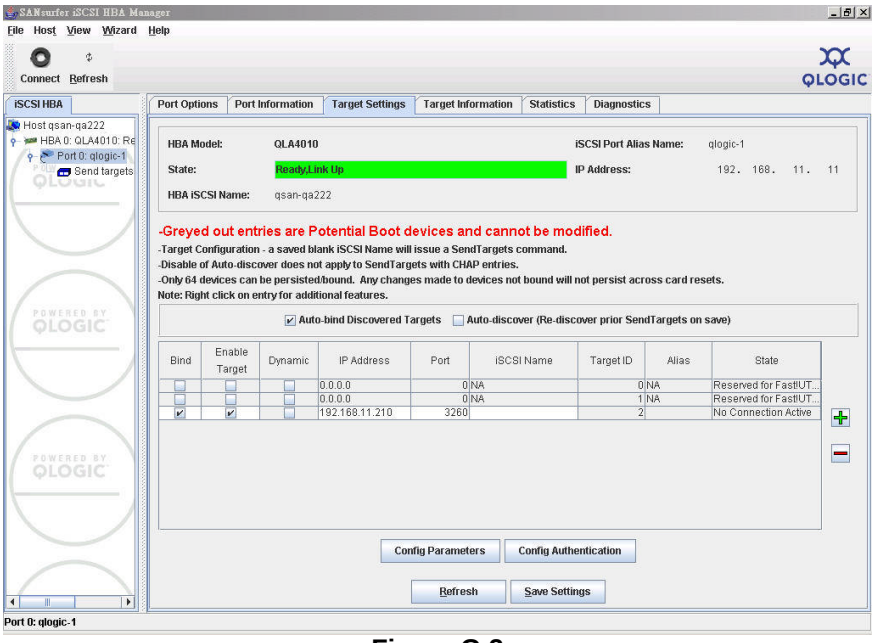


Figure G.2

3. Disable **“Immediate Data”** and enable **“Initial R2T”**.

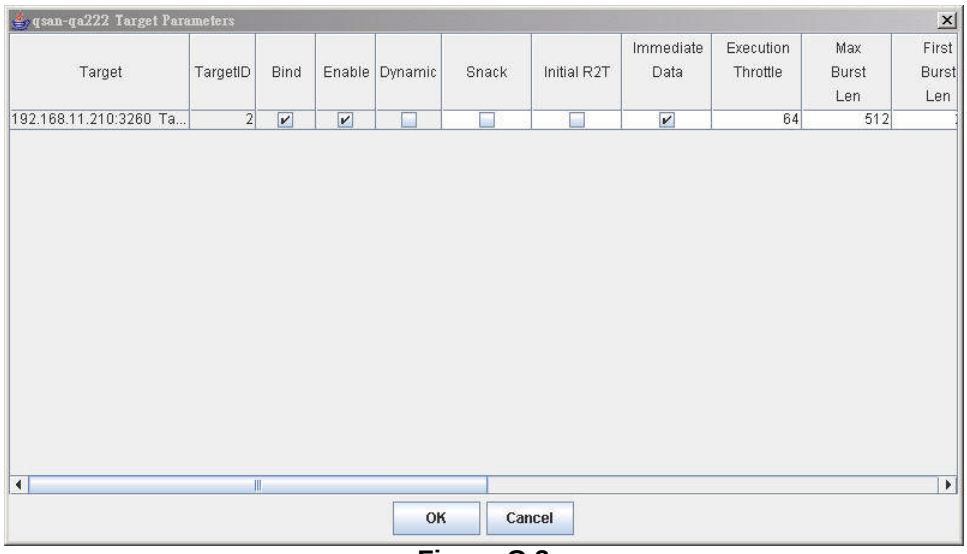


Figure G.3

4. Click **“OK”**.

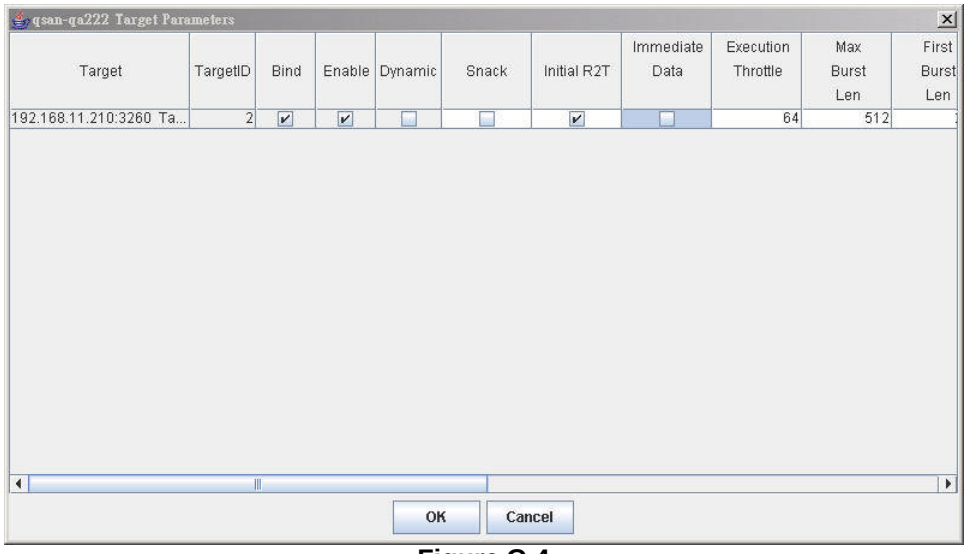


Figure G.4

5. Click **“Save settings”** and click **“Yes”** on next page.

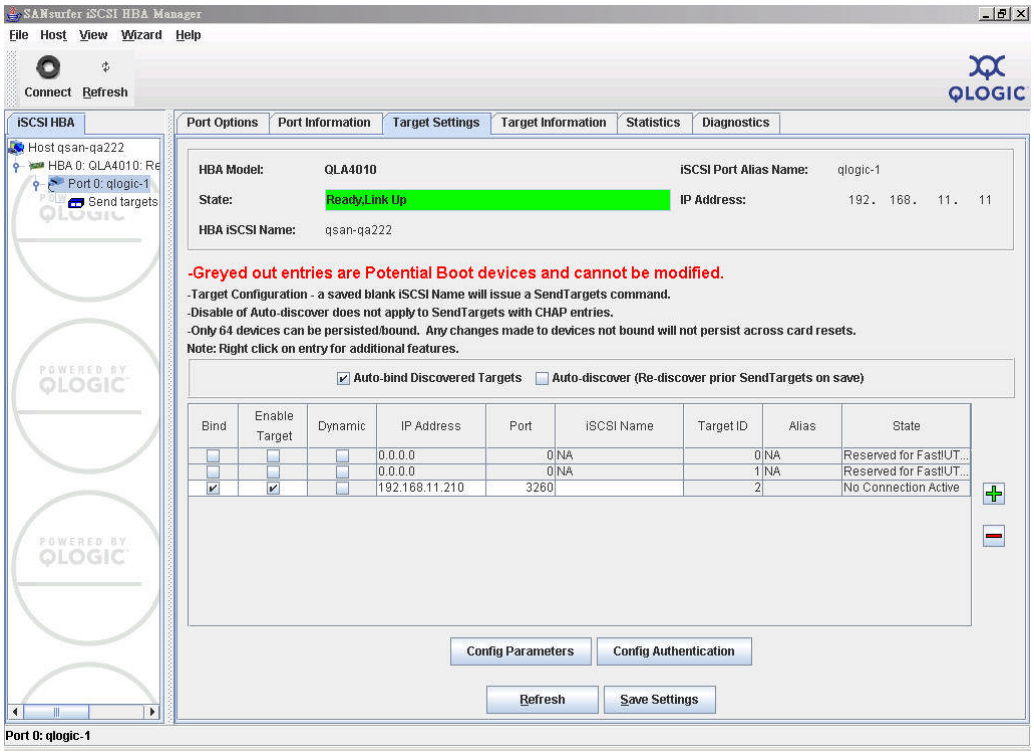


Figure G.5

6. Click **“Refresh”** and find a new target with iSCSI name.

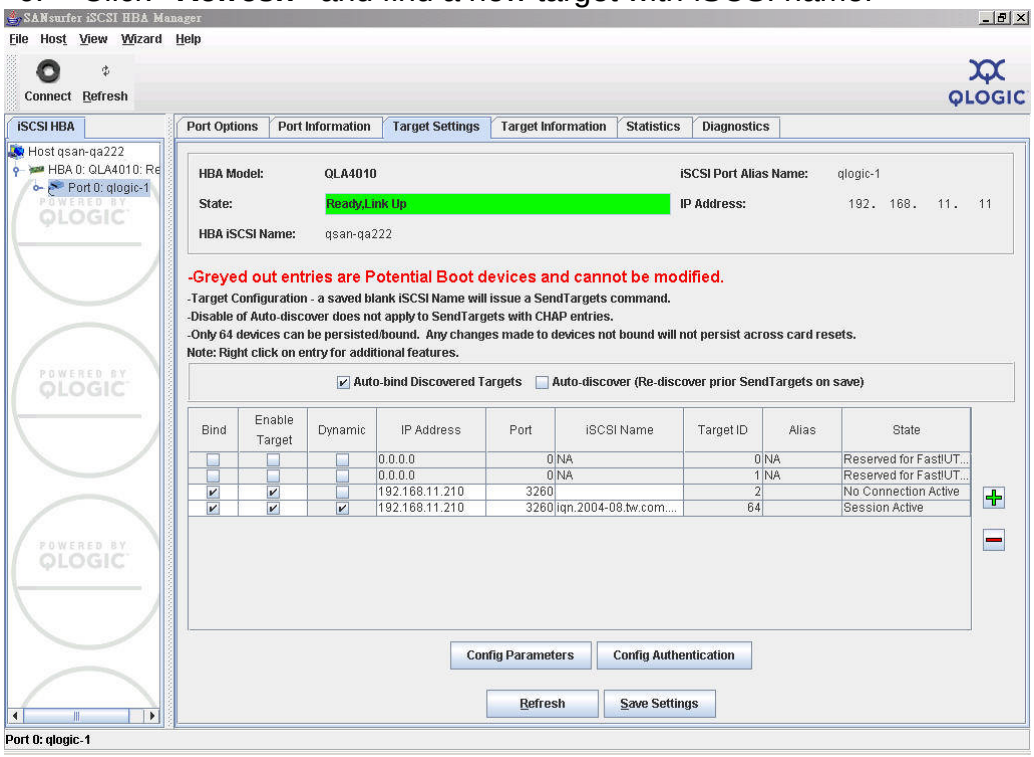

SANsurfer iSCSI HBA Manager
File Host View Wizard Help
Connect Refresh
QLOGIC
iSCSI HBA
Host qsan-qa222
HBA 0: QLA4010: Re
Port 0: qlogic-1
Port Options
Port Information
Target Settings
Target Information
Statistics
Diagnostics
HBA Model: QLA4010
iSCSI Port Alias Name: qlogic-1
State: Ready,Link Up
IP Address: 192. 168. 11. 11
HBA iSCSI Name: qsan-qa222
-Greyed out entries are Potential Boot devices and cannot be modified.
-Target Configuration - a saved blank iSCSI Name will issue a SendTargets command.
-Disable of Auto-discover does not apply to SendTargets with CHAP entries.
-Only 64 devices can be persisted/bound. Any changes made to devices not bound will not persist across card resets.
Note: Right click on entry for additional features.
Auto-bind Discovered Targets
Auto-discover (Re-discover prior SendTargets on save)
Bind
Enable Target
Dynamic
IP Address
Port
iSCSI Name
Target ID
Alias
State
0.0.0.0 0 NA 0 NA Reserved for FastIUT...
0.0.0.0 0 NA 1 NA Reserved for FastIUT...
192.168.11.210 3260 2 No Connection Active
192.168.11.210 3260 iqn.2004-08.tw.com.... 64 Session Active
Config Parameters
Config Authentication
Refresh
Save Settings
Port 0: qlogic-1

Figure G.6

7. Check the parameters. **“Initial R2T”** are must be enabled.

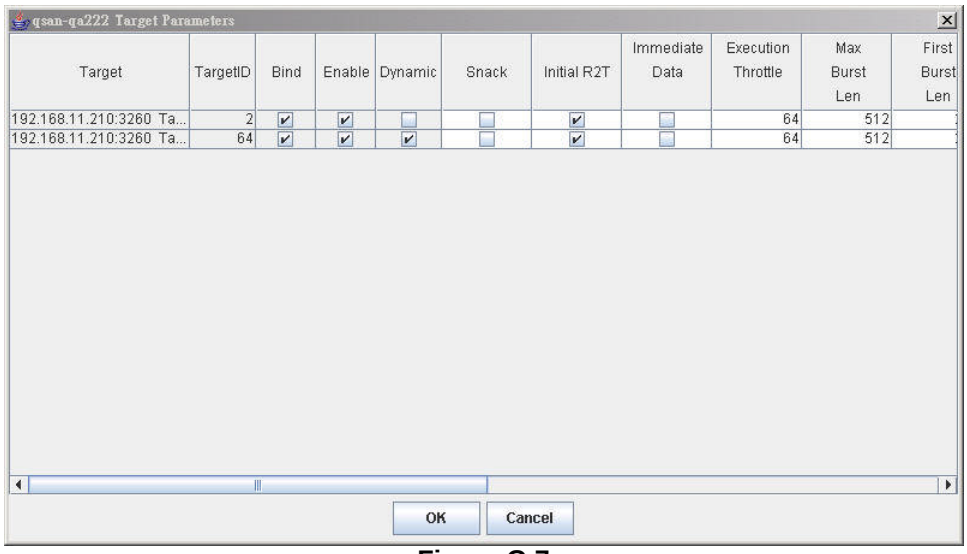


Figure G.7

8. Check **“Target Information”** again and the state changed to **“Session Active”**.

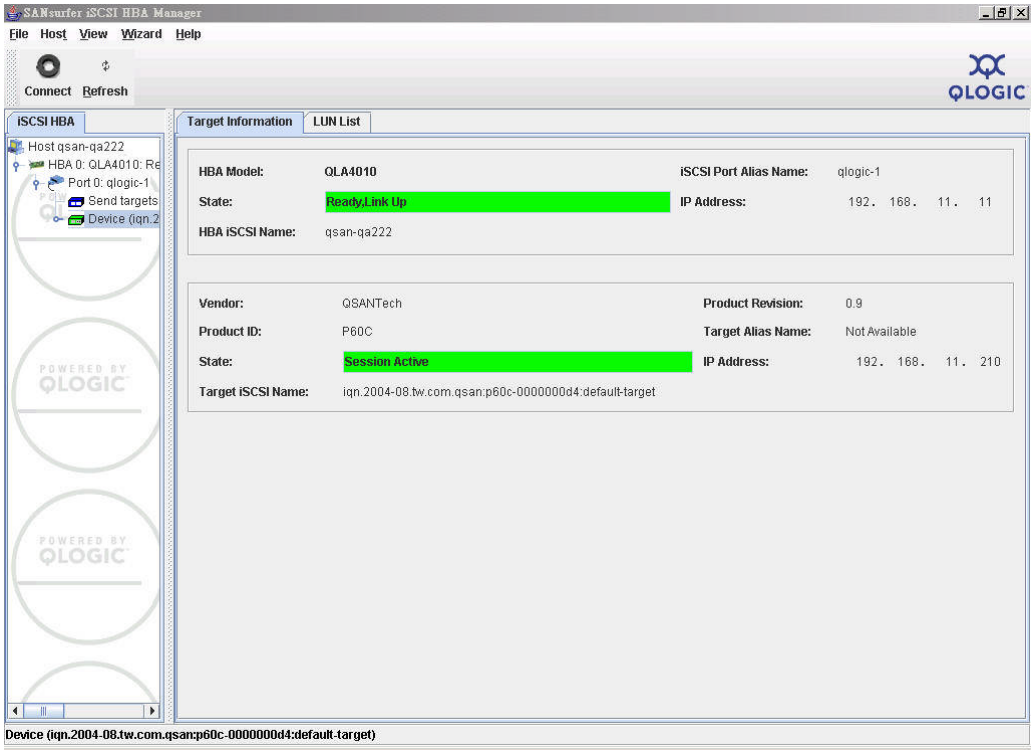


Figure G.8

9. Then, run **“Computer Management”** in Windows. Make sure the disk appears.

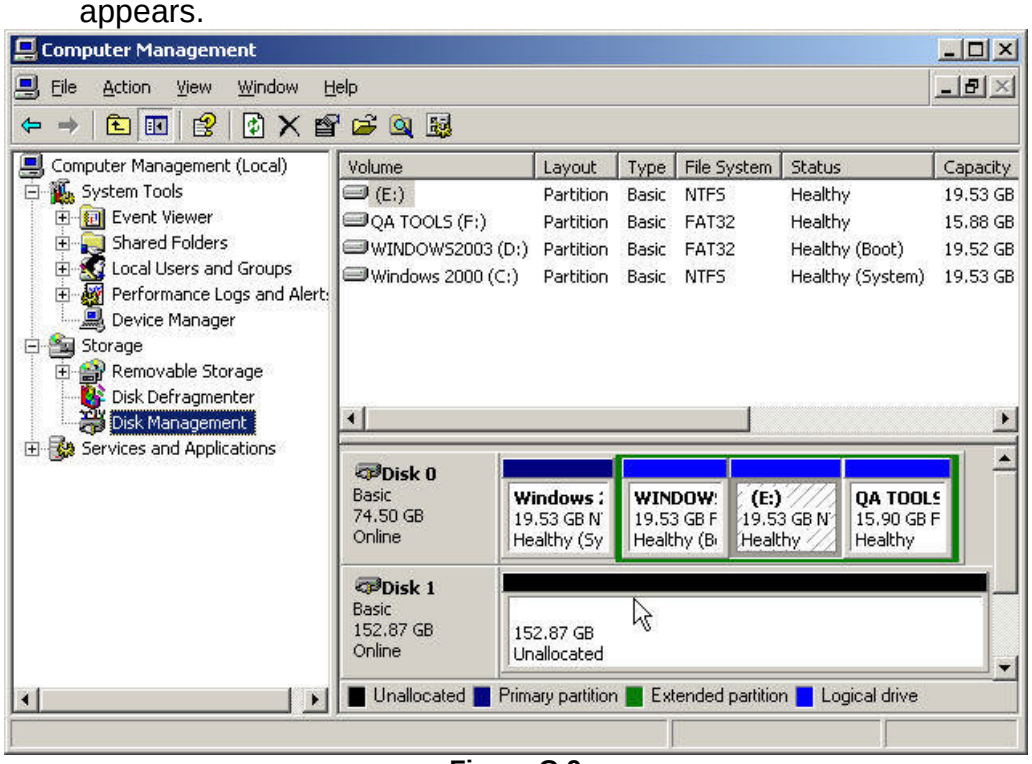


Figure G.9

G. Installation Steps for Large Volume (TB)

Introduction:

The ISC8P2G is capable of supporting large volumes (>2TB). When connecting controllers to 64bit OS installed host/server, the host/server is inherently capable for large volumes from the 64bit address. On the other side, if the host/server is installed with 32bit OS, user has to change the block size to 1KB, 2KB or 4KB to support volumes up to 4TB, 8TB or 16TB, for the 32bit host/server is not LBA (Logical Block Addressing) 64-bit supported. For detailed installation steps, check below.

Step A: configure your target

1. Go to **/ Volume config / Volume group**, create a VG.

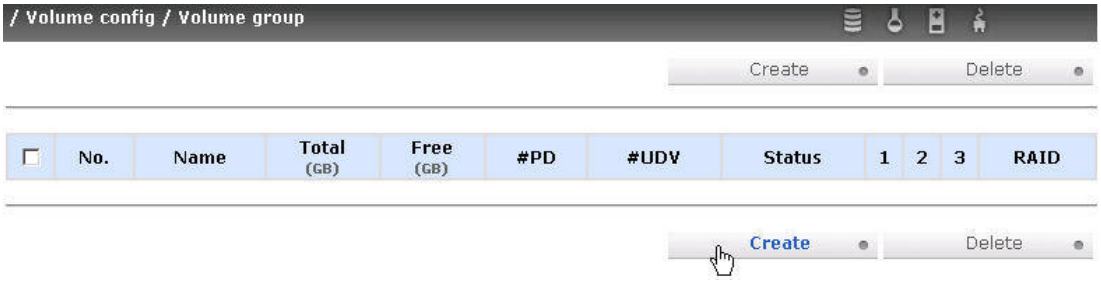


Figure H.1

2. Choose RAID level and disks.

Figure H.2

3. Confirm VG settings.

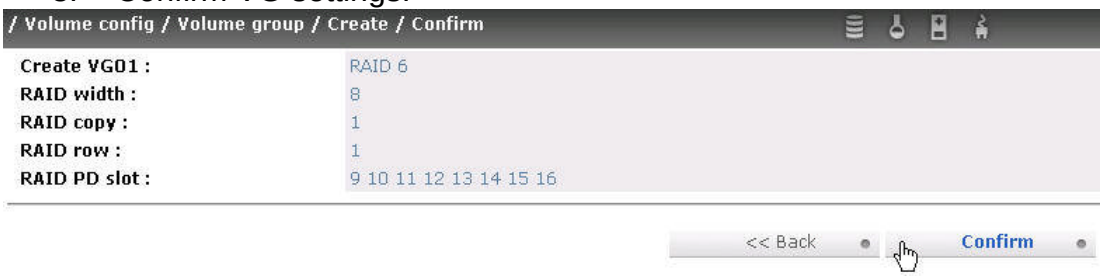


Figure H.3

4. A RAID 6 VG is created.

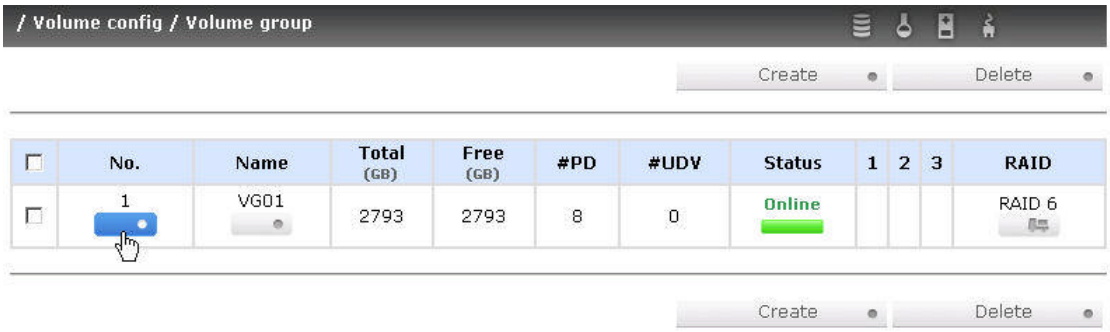


Figure H.4

5. Go to **/ Volume config / User data volume**, create a UDV

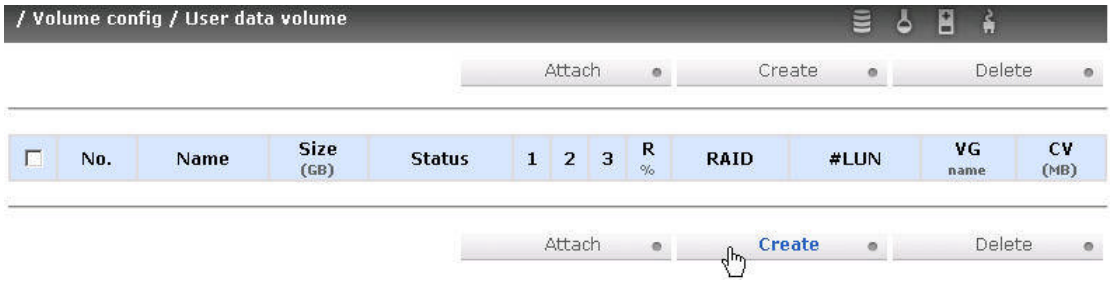


Figure H.5

6. Setup capacity, stripe height, and block size for UDV.

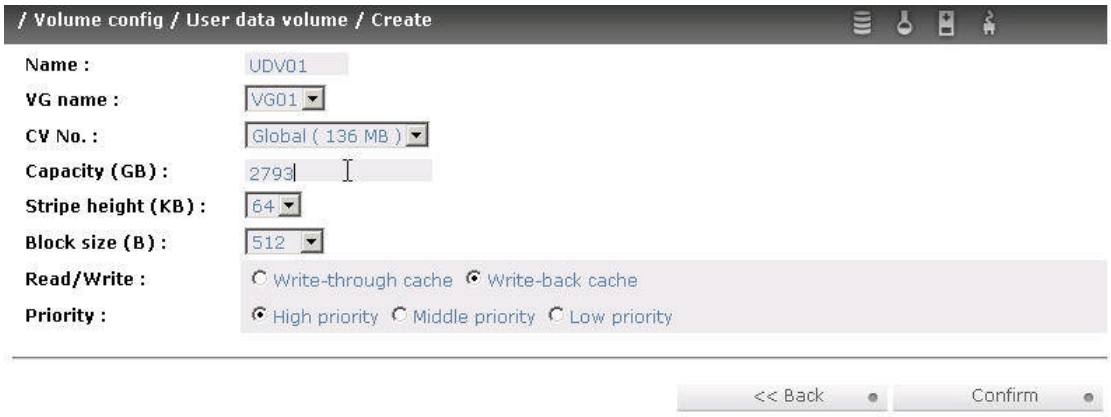


Figure H.6

Tips

When the OS is 64bit, user can set the block size to any available value. If the OS is 32bit, user must change the block size to values larger than 512B. There will be a confirmation pop-up when UDV size is over 2TB.

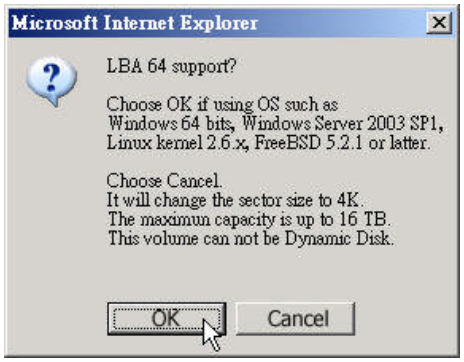

Microsoft Internet Explorer
LBA 64 support?
Choose OK if using OS such as
Windows 64 bits, Windows Server 2003 SP1,
Linux kernel 2.6.x, FreeBSD 5.2.1 or latter.
Choose Cancel.
It will change the sector size to 4K.
The maximun capacity is up to 16 TB.
This volume can not be Dynamic Disk.
OK
Cancel

Figure H.7:

(Figure H.7: choose "OK" for 64bit OS, choose "Cancel" for 32bit OS, this step will change block size to 4K automatically.)

7. A 2.793TB UDV is created.

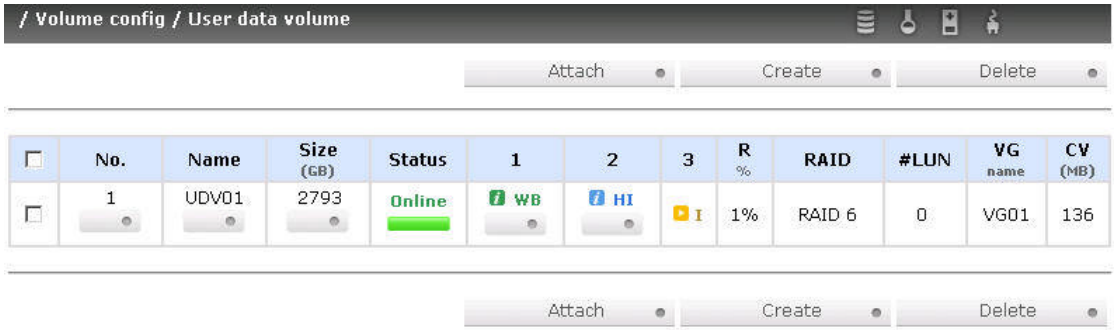


Figure H.8: a 2793G UDV is created.

8. Check the detail information.

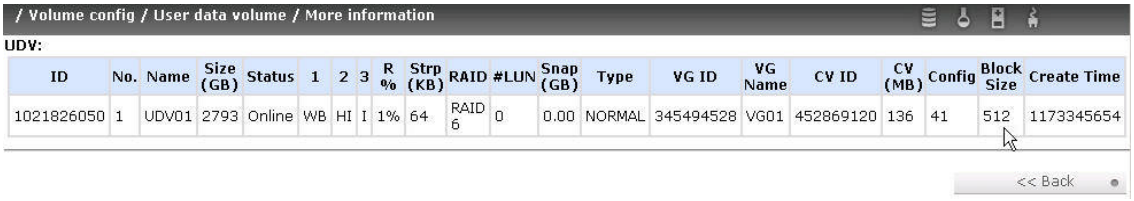


Figure H.9

(Figure H.9: block size = 512B, for 64bit OS setting.)

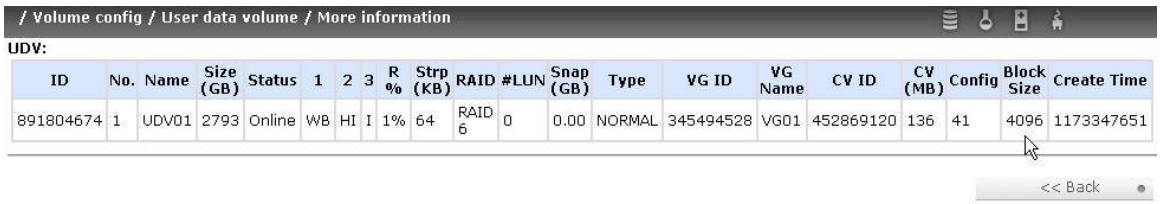


Figure H.10

(Figure H.10: block size = 4K, for 32bit OS setting.)

9. Attach LUN.

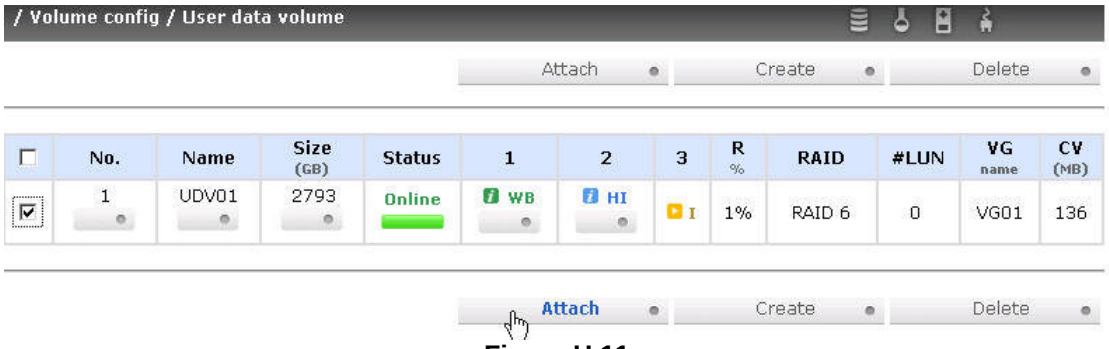


Figure H.11

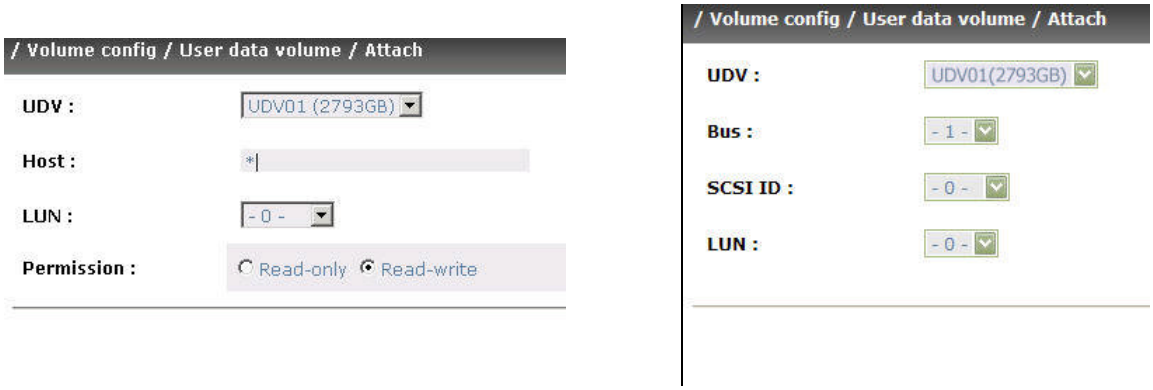


Figure H.12

(Figure H.12: Left: P series; Right: S series attach LUN.)

Step B: configure your host/server

1. You need to setup software iscsi initiator or iSCSI HBA first.

2. Below is the configuration for Windows Server 2003 R2 with Microsoft iscsi initiator. Please install the latest Microsoft iscsi initiator from the link below.
   http://www.microsoft.com/downloads/details.aspx?FamilyID=12cb3c1a-15d6-4585-b385-befd1319f825&DisplayLang=en

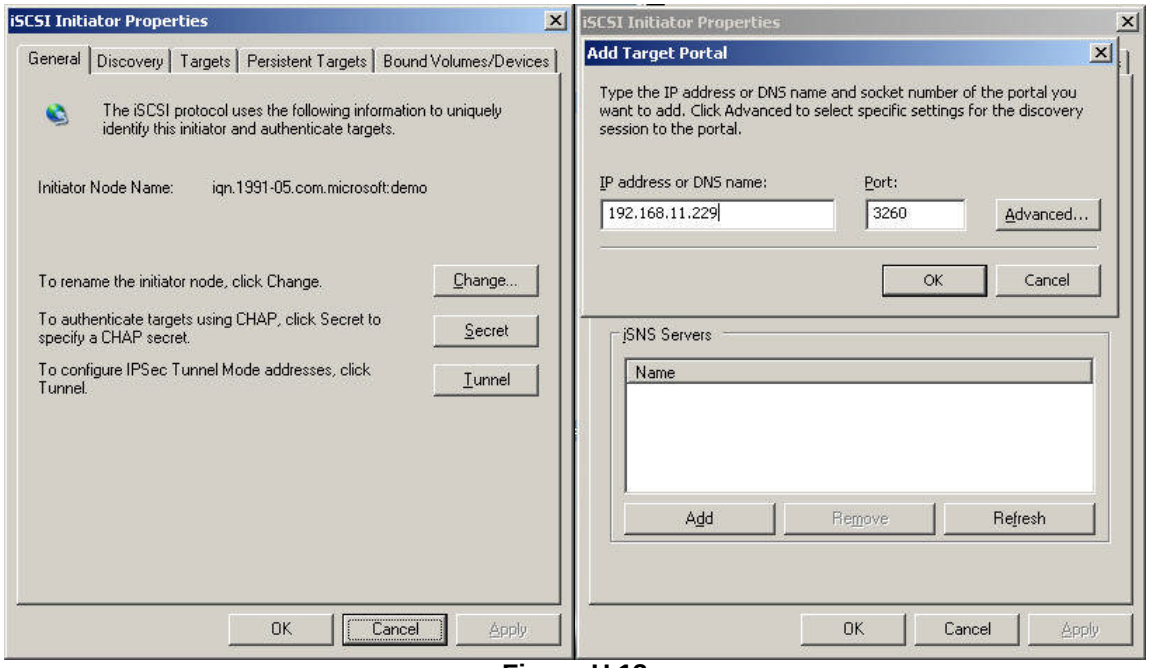


Figure H.13

(Figure H.13: Run MS iSCSI initiator, go to “Discovery” tab, add target portal (iSCSI data).)

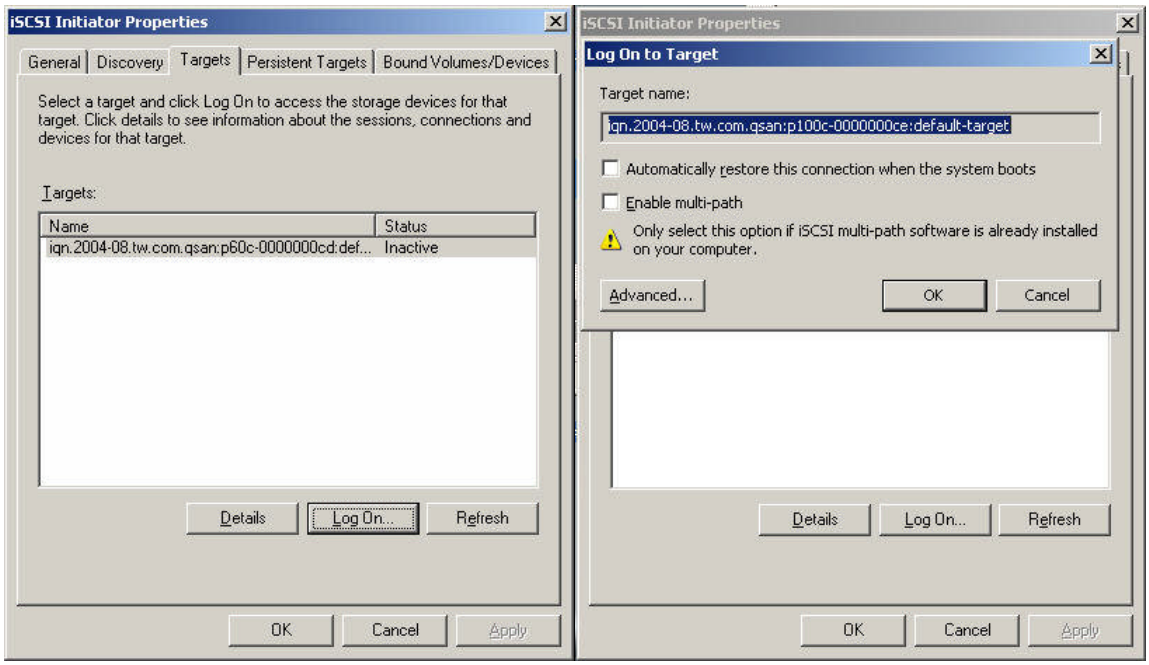


Figure H.14

(Figure H.14: go to “Targets” tab, click “Refresh”, and then “Log On…” the target.)

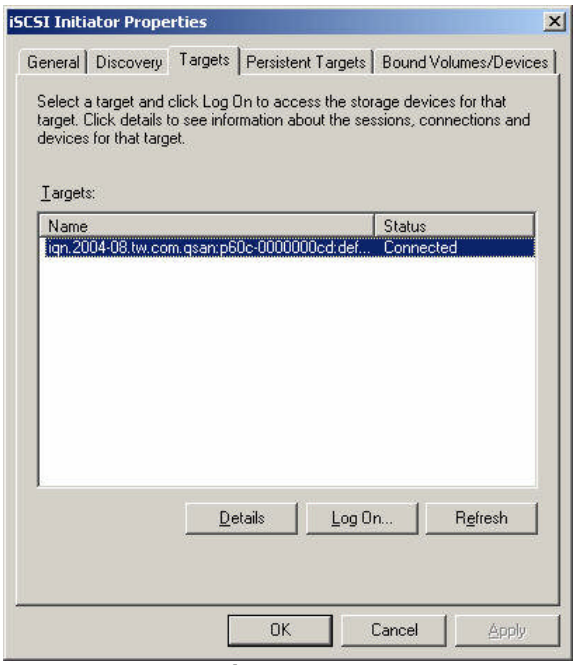


Figure H.15

(Figure H.15: Status is “Connected”, the initiator setting is done.)

Step C: Initialize/Format/Mount the disk

1. Go to Start à Control Panel à Computer Management à Device Manger à Disk drives

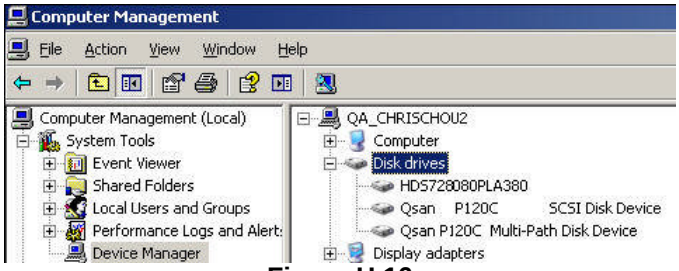


Figure H.16

(Figure H.16: Disk drive status of ISC8P2G.)

2. Go to Start à Control Panel à Computer Management à Disk Management, it displays a new disk.

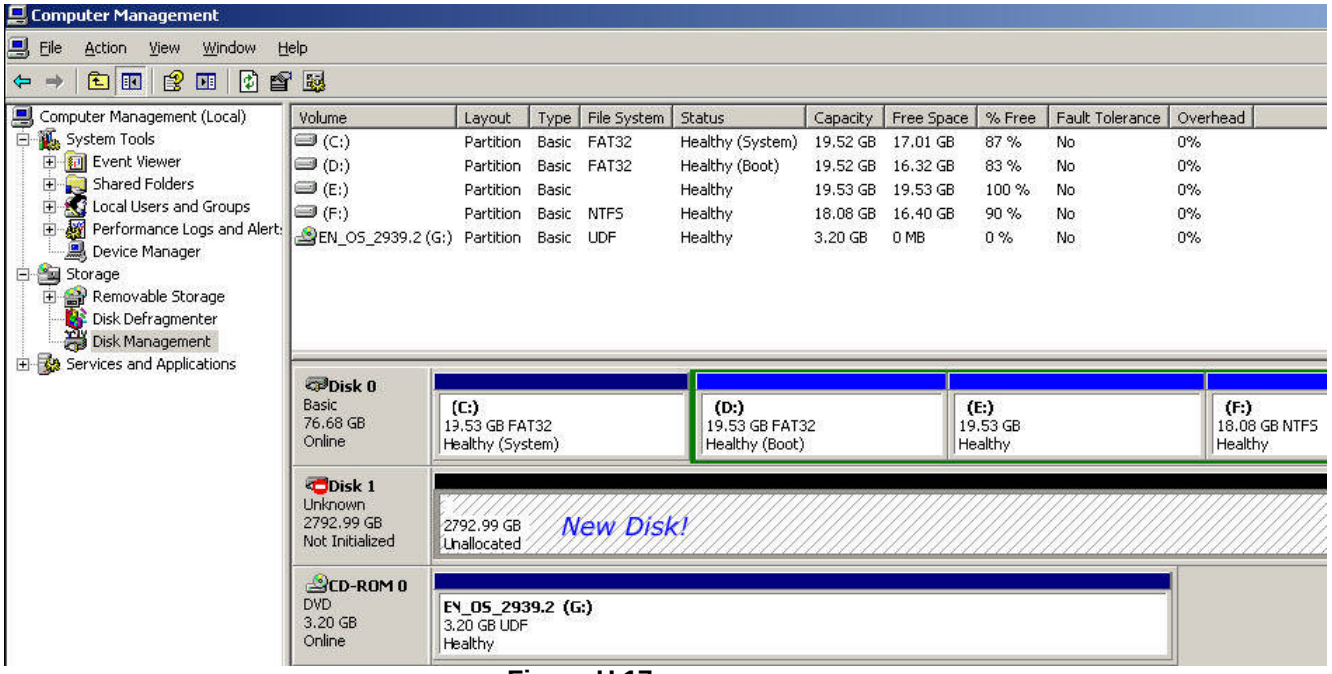


Figure H.17

3. Initialize disk.

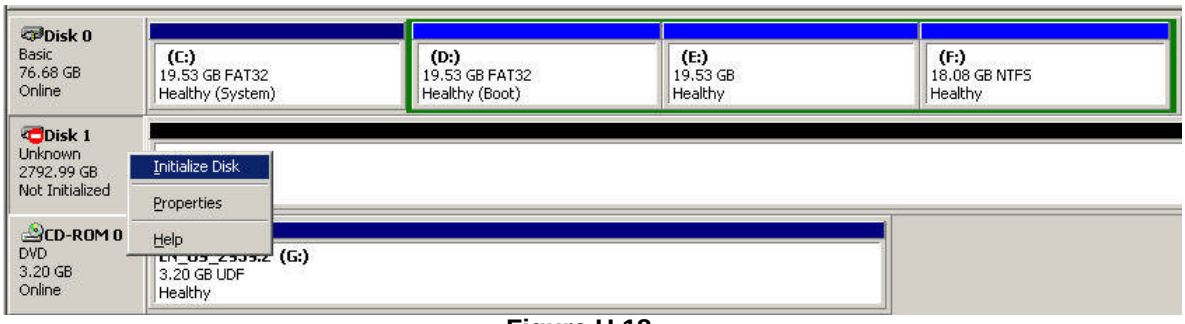


Figure H.18

4. Convert to GPT disk for over 2TB capacity. For more detail information about GPT, please visit **http://www.microsoft.com/whdc/device/storage/GPT_FAQ.mspx**

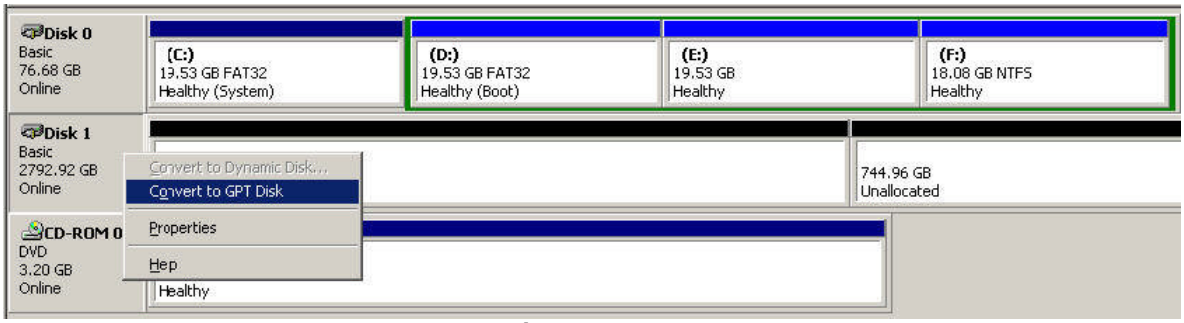


Figure H.19

5. Format disk.

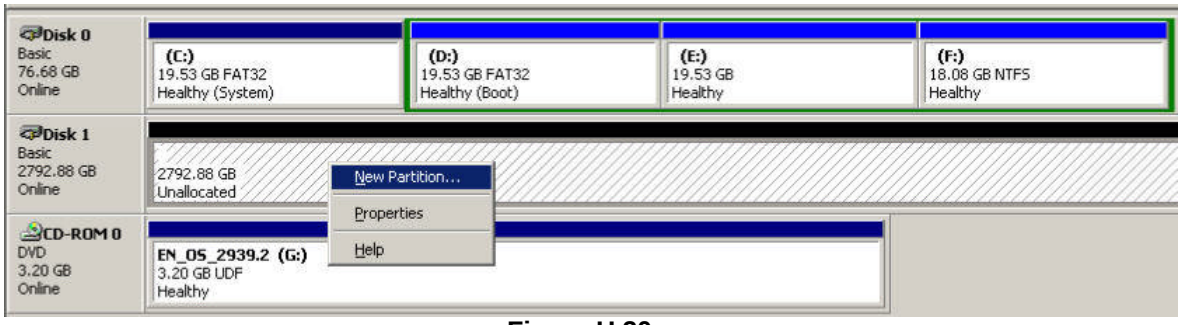


Figure H.20

6. Format disk is done.

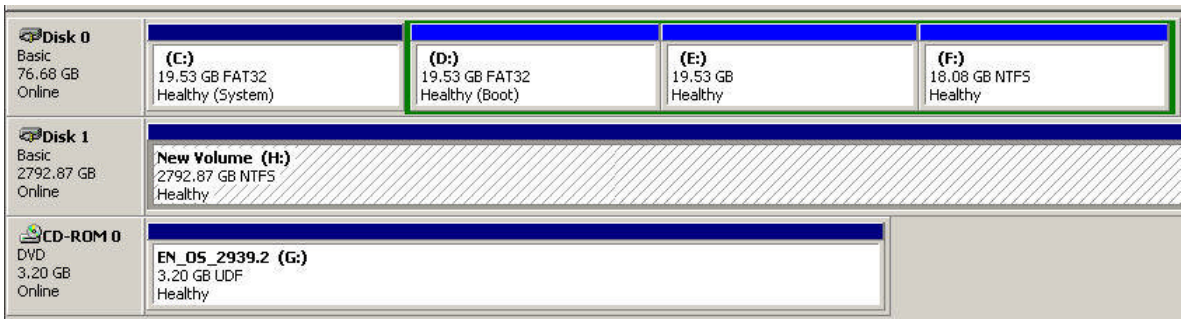


Figure H.21

7. The new disk is ready, available size = 2.72TB.

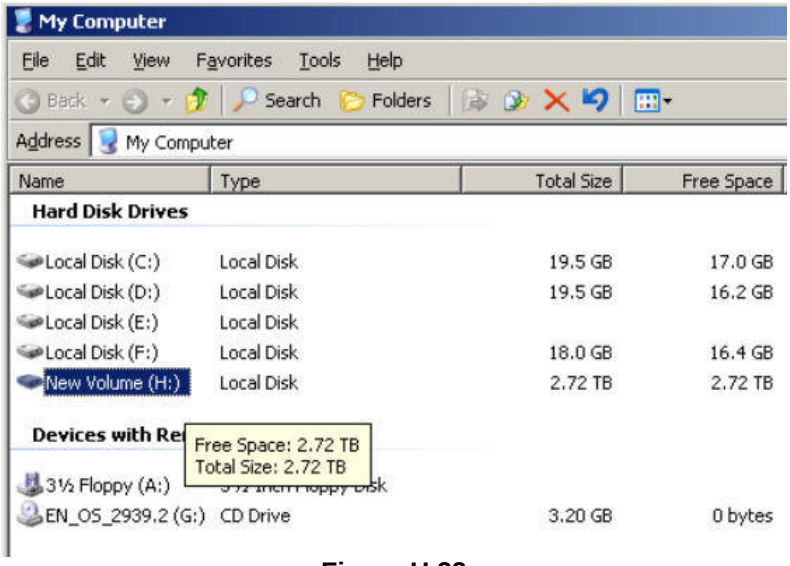

My Computer
File Edit View Favorites Tools Help
Back Search Folders
Address My Computer
Name Type Total Size Free Space
Hard Disk Drives
Local Disk (C:) Local Disk 19.5 GB 17.0 GB
Local Disk (D:) Local Disk 19.5 GB 16.2 GB
Local Disk (E:) Local Disk
Local Disk (F:) Local Disk 18.0 GB 16.4 GB
New Volume (H:) Local Disk 2.72 TB 2.72 TB
Free Space: 2.72 TB
Total Size: 2.72 TB
3½ Floppy (A:)
EN_OS_2939.2 (G:) CD Drive 3.20 GB 0 bytes

Figure H.22

Caution
If the user has setup 512B as block size for UDV and the host/server OS is 32bit, in the last step of formatting disk, user will find OS cannot format the area after 2048GB (2TB).

8. Wrong setting result: OS cannot format area after 2048GB(2TB).

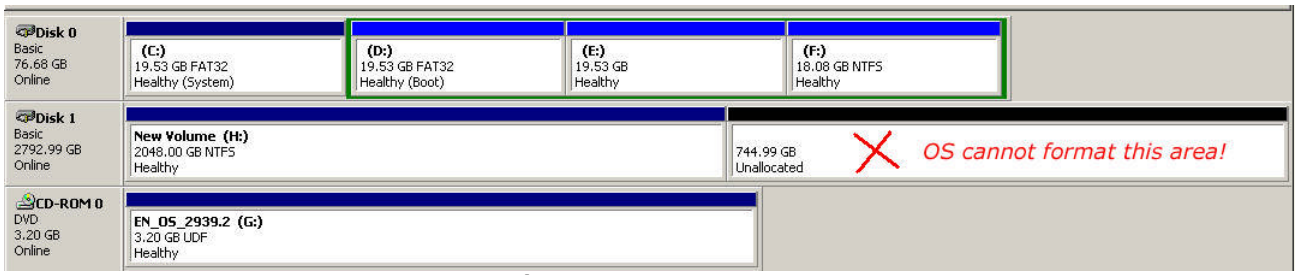


Figure H.23